Symantec™ Network Security Installation Guide 4.0

Symantec Network Security 4.0 Installation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 4.0

PN: 10325006

Copyright Notice

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

Trademarks

Symantec, the Symantec logo, LiveUpdate, ManHunt, Symantec Decoy Server, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. Symantec AntiVirus, Symantec Enterprise Security Architecture, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Windows is a registered trademark, and 95, 98, NT and 2002 are trademarks of Microsoft Corporation. Pentium is a registered trademark of Intel Corporation. Sun is a registered trademark, and Java, Solaris, Ultra, Enterprise, and SPARC are trademarks of Sun Microsystems. UNIX is a registered trademark of UNIX System Laboratories, Inc. Cisco and Catalyst are registered trademarks of Cisco Systems, Inc. Foundry is a registered trademark of Foundry Networks. Juniper is a registered trademark of Juniper Networks, Inc. iButton is a trademark of Dallas Semiconductor Corp. Dell is a registered trademark of Dell Computer Corporation. Check Point and OPSEC are trademarks and FireWall-1 is a registered trademark of Check Point Software Technologies, Ltd. Oracle is a registered trademark and Oracle is a trademark of Oracle Corporation. Tripwire is a registered trademark of Tripwire, Inc.

Symantec ManHunt software contains/includes the following Third Party Software from external sources: “bzip2” and associated library “libbzip2,” Copyright © 1996-1998, Julian R Seward. All rights reserved. Oracle JDBC Drivers 8.1.7. Copyright © Oracle Corporation.

Printed in the United States of America. 10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

See "About Symantec licenses" on page 71.

Contacting Technical Support

Customers with a current support agreement may contact the Symantec global Technical Support group by phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information

- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to **www.symantec.com**, select the appropriate Global Site for your country, then choose Service and Support.

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC SOFTWARE LICENSE AGREEMENT
SYMANTEC NETWORK SECURITY

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License.

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use the number of copies of the Software as have been licensed to You by Symantec under a License Module. If the Software is part of a suite containing multiple Software titles, the number of copies You may use may not exceed the aggregate number of copies indicated in the License Module, as calculated by any combination of licensed Software titles. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single computer;

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;

D. use the Software in accordance with any written agreement between You and Symantec; and

E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees in writing to the terms of this license.

You may not:

A. copy the printed documentation that accompanies the Software;

B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;

D. use a previous version or copy of the Software after You have received and installed a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

E. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received permission in a License Module; nor

G. use the Software in any manner not authorized by this license.

H. use the Software in any manner that contradicts any additional restrictions set forth in Section 8, below.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of thirty (30) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. Licensee agrees to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. Licensee agrees not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, Licensee agrees not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will it sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland , or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

8. Additional Uses and Restrictions:

If the Product you have licensed is Symantec Network Security, the following additional terms apply:

A. You may not create additional classes, interfaces, or subpackages that are contained in the "java" or "sun" packages or similar as specified by Sun Microsystems in any class file naming convention.

B. Symantec suppliers and licensors, including Oracle Corporation, are third-party beneficiaries of provisions of this Agreement that relate to third party software, a supplier, or portions of the Software furnished by such suppliers.

C. You may only use the number of iButton devices as set forth in the applicable License Module. Otherwise, You have no rights to use the iButton device. You must separately purchase applicable maintenance and support for the iButton device.

Contents

Chapter 1 Introduction

Chapter 2 System requirements

Chapter 3 Installation

Chapter 4 Post-installation

Chapter 5 Upgrading

Appendix A Integrating with SESA

Appendix B Using iButtons

Appendix C Reimaging iForce

Index

Chapter 1

Introduction

This chapter includes the following topics:

- About Symantec™ Network Security
- About the Symantec™ Network Security Management Console
- Finding information

About Symantec™ Network Security

Symantec Network Security is a new generation of security software that provides an unprecedented ability to detect, analyze, and respond to network intrusions and prevent damage from attacks. It reduces the total cost of implementing a complete network security solution by providing simplified and rapid deployment, centralized management, and cohesive and streamlined security content, service, and support.

Symantec Network Security complements the Symantec Network Security 7100 Series, a family of highly scalable, integrated hardware and software intrusion detection appliances, designed to detect and prevent attacks across multiple network segments at multi-gigabit speeds.

This Guide introduces you to the Symantec Network Security management system, describes how to install the core Symantec Network Security software, and outlines how to make initial setup and configuration decisions.

This section includes the following topics:

- About detection
- About analysis
- About response
- About deployment

About detection

Symantec Network Security provides hybrid detection architecture using an array of detection methodologies for effective attack detection and accurate attack identification. It collects evidence of malicious activity with a combination of protocol anomaly detection, stateful signatures, event refinement, traffic rate monitoring, IDS evasion handling, flow policy violation, IP fragmentation reassembly, and user-defined signatures.

Symantec Network Security sets new standards with multi-gigabit, high-speed traffic monitoring allowing implementation at virtually any level within an organization, even on gigabit backbones. On a certified platform, Symantec Network Security can maintain 100% of its detection capability at 2Gbps across 6 gigabit network interfaces with no packet loss.

Symantec Network Security's protocol anomaly detection helps detect previously unknown and new attacks as they occur. This capability, dubbed “zero-day” detection, closes the window of vulnerability inherent in signature-based systems that leave networks exposed until signatures are published.

Predefined policies speed deployment by allowing you to quickly configure immediate responses to intrusions or denial-of-service attacks, based on the type and the location of the event within the network. Independently configurable detection settings make it easy for you to create granular responses that are customized to the needs of your particular environment. You can apply policies at the cluster, node, or interface level for complete, scalable control.

About detection architecture

The Symantec Network Security solution provides comprehensive security protection and proactive risk mitigation. At the heart of this solution lies the detection architecture. Symantec Network Security provides state-of-the-art protection against both today’s and tomorrow’s blended and complex threats. It combines multiple detection technologies such as protocol anomaly detection, vulnerability attack interception, signature detection, denial-of-service and scan detection, IDS evasion detection, and traffic monitoring, to accurately identify and mitigate attacks.

About analysis

Symantec Network Security's correlation and analysis engine filters out redundant data and analyzes only the relevant information, providing threat awareness without data overload. Symantec Network Security gathers intelligence across the enterprise using cross-node analysis to quickly spot trends and identify related events and incidents as they happen. In addition, new user-configurable correlation rules enable users to tune correlation performance to meet the needs of their own organization and environment.

You can configure full-packet capture, session playback, and flow querying capabilities on a per-interface basis to capture the entire packet when an attack is detected so that you can quickly determine if the offending packet is a benign event that can be filtered or flagged for further investigation. Automated response actions can initiate traffic recording and flow exports, and you can query existing or saved flows, as well as playback saved sessions to further assist in drill-down analysis of a security event.

About response

Proactive response rules contain and control the attack in real-time, and initiate other actions required for incident response. Customized policies provide immediate response to intrusions or denial-of-service attacks, based on the type and the location of the event within the network. Symantec Network Security implements session termination, traffic recording and playback, flow export and query, TrackBack, and custom responses, combined with email and SNMP notifications, to protect an enterprise's most critical assets.

About deployment

Symantec Network Security provides cost-effective scalable deployment whereby a single Network Security software node can monitor multiple segments or VLANs. Each node can be configured to monitor up to 12 Fast Ethernet ports or 6 to 8 Gigabit Ethernet ports. As the network infrastructure grows, network interface cards can be added to the same node to support additional monitoring requirements.

Symantec Network Security also supports high availability deployment (H/A) to ensure continuous attack detection without any loss of traffic or flow data in your mission-critical environment.

About centralized cluster management

The full power and advanced features of Symantec Network Security become available when you create a group or cluster of nodes, and establish one node as the master. A Symantec Network Security deployment can consist of multiple clusters, each cluster consisting of up to 120 nodes.

An entire Network Security cluster can be securely and remotely managed from a centralized management console. The Network Security console provides complete cluster topology and policy management, node and sensor management, incident and event monitoring, and drill-down incident analysis and reporting.

For more information about clusters and advanced cluster management, see the *Symantec Network Security Administration Guide*.

About the Symantec™ Network Security Management Console

Symantec Network Security is centrally managed from the Symantec™ Network Security Management Console (Network Security console), a powerful and scalable security management system that supports large, distributed enterprise deployments. The Network Security console provides comprehensive configuration and policy management, real-time threat analysis, enterprise reporting, and flexible visualization.

The Network Security console provides a centralized location from which you can administer all nodes in the cluster, both master and slave. From this single interface, you can view all attack activity being logged by any node in the cluster. You can set up, configure, and perform maintenance and adjustment tasks from the console, including updating the topology database, defining detection policies and response rules, and so on. These actions are propagated to the other nodes in the cluster.

The Network Security console supports role-based administration—the ability to define administrative users and assign them roles with varying levels of access rights. Administrative users can be assigned roles all the way from the full range of SuperUser privileges, down to the most limited RestrictedUser access, allowing only event monitoring without packet inspection capabilities. All administrative changes made from the Network Security console are logged for auditing purposes.

Finding information

This section describes the organization of this Guide, how to find additional information about Symantec Network Security, and how to contact Technical Support:

- About the organization of this guide
- About additional Symantec Network Security documentation
- About support

About the organization of this guide

This Guide contains the following:

- Chapter 1 Introduction: Provides an overview of the Symantec Network Security software and of this Guide, including how to find the information you need, technical support, and additional information.
- Chapter 2 System requirements: Provides a summary of the system requirements for the Symantec Network Security software, described in more detail in the *Hardware Compatibility Reference*.
- Chapter 3 Installation: Describes the installation procedure and installation options for Symantec Network Security.
- Chapter 4 Post-installation: Describes optional post-installation procedures, such as hardening the system, adding NICs and tokens, and integrating other Symantec products such as SESA and DeepSight.
- Chapter 5 Upgrading: Describes the upgrade and migration options available for the Symantec Network Security software and for components such as NICs, tokens, and databases, as well as specialized procedures for upgrading clusters.
- Chapter 6 Licensing: Describes the licensing options available for the Symantec Network Security software.
- Chapter 7 LiveUpdating: Describes the LiveUpdate options available for the Symantec Network Security software so that you always have the latest Security Updates, Product Updates, and Engine Updates.
- Appendix A Integrating with SESA: Describes how to integrate your Symantec Network Security system with the Symantec Enterprise Security Architecture (SESA) and install the SESA Bridge.
- Appendix B Using iButtons: Describes how to install, uninstall, manage and troubleshoot software tokens and iButtons on your Symantec Network Security system.
- Appendix C Reimaging iForce: Describes the procedures for reinstalling iForce in an emergency.

About additional Symantec Network Security documentation

The documentation set for Symantec Network Security core software includes:

- *Symantec Network Security Getting Started* (printed and PDF): This guide provides basic introductory information about the Symantec Network Security software product, an abbreviated list of system requirements, and a basic checklist for getting started.

- *Symantec Network Security Installation Guide* (printed and PDF): This guide explains how to install, upgrade, and migrate Symantec Network Security software on supported platforms.
- *Symantec Network Security Administration Guide* (printed and PDF): This guide provides the main reference material, including detailed descriptions of the Symantec Network Security features, infrastructure, and how to configure and manage the detection system effectively.
- *Symantec Network Security Signature Developers' Guide* (Web only): This Guide contains detailed descriptions of the proprietary Symantec Network Security Signature Language and how to use it to create effective user-defined signatures to customize the detection system.
- *Symantec Network Security User Guide* (PDF): This guide provides introductory information about Symantec Network Security core software for the user with read-only access.
- *Symantec Network Security Readme* (on CD): This document provides late-breaking information about Symantec Network Security core software, limitations and workarounds.
- *Symantec Network Security Hardware Compatibility Reference* (Web only): This reference contains the most up-to-date lists of supported hardware platforms, operating systems, NICs, and chipsets, as well as specialized installation instructions.

About support

From the Symantec Network Security Web site you can view the entire documentation set, as well as the continually updated Hardware Compatibility Reference, Knowledge Base, and patch Web sites.

Calling for help

Customers with a current support agreement may contact the Symantec global Technical Support group by phone or online at www.symantec.com/techsupp.

See also “Contacting Technical Support” on page 3.

About the Knowledge Base

The *Knowledge Base* provides a continuously updated reference of FAQs and troubleshooting tips as they are developed. You can view the *Knowledge Base* on the Symantec Network Security Web site.

To view the Knowledge Base

1. Open the following URL:
   www.symantec.com/techsupp/enterprise/select_product_kb.html
2. Click **Intrusion Protection** > **Symantec Network Security 4.0**.
3. Do one of the following:
   - View a list of articles on the Hot Topics tab. Click an article to view it.
   - On the Search tab, enter the search criteria, then click **search**.
   - On the Browse tab, expand a category to see each type. Click a topic to view a list of articles. Click an article to view it.

About the Hardware Compatibility Reference

The *Symantec Network Security Hardware Compatibility Reference* provides a detailed list of platforms supported by Symantec Network Security. You can view the Hardware Compatibility Reference on the Symantec Network Security Web site.

To view the Hardware Compatibility Reference

1. Open the following URL:
   www.symantec.com/techsupp/enterprise/select_product_manuals.html
2. Click **Intrusion Protection** > **Symantec Network Security 4.0**.

About the Product Updates site

The *Product Update Site* references product updates (patches) as they are released. Product updates, signature updates, and engine updates are now released via LiveUpdate. You can view the available product update documentation on the Symantec Network Security Web site.

To view the Product Update Site

1. Open the following URL:
   www.symantec.com/techsupp/enterprise/select_product_updates.html
2. Click **Intrusion Protection** > **Symantec Network Security 4.0**.

About Symantec Network Security documentation

You can view all Symantec Network Security documentation on the Symantec Network Security Web site.

To view all documentation

1. Open the following URL:
   www.symantec.com/techsupp/enterprise/select_product_manuals.html
2. Click **Intrusion Protection** > **Symantec Network Security 4.0**.

Chapter 2

System requirements

This chapter includes the following topics:

- About node requirements
- About Network Security console requirements
- About requirements for optional functionality

About node requirements

This section provides an overview of the basic hardware, system, and memory requirements for the Symantec Network Security software. The requirements are described in more detail in the *Symantec Network Security Hardware Compatibility Reference*.

See "About the Hardware Compatibility Reference" on page 17.

This section includes the following topics:

- About hardware requirements
- About operating system requirements
- About memory requirements

About hardware requirements

Symantec Network Security software requires a dedicated multiple-CPU computer separate from the Network Security console, on a supported Sun® SPARC™ or x86 platform. Consider the volume of traffic to monitor and the characteristics of the network configuration when you select the hardware.

Place the Network Security software node in the same location as the routers and other network devices carrying the traffic that the node will monitor. If possible, place the node in the same racks.

Each node has a primary network interface for both administration, management, and communication with other nodes and network devices. For optimal performance, one Network Interface Card (NIC) for each monitored device (up to 12 Fast Ethernet or 6 gigabit Ethernet) is installed in the host computer, including gigabit interfaces to monitor gigabit links. The number of additional interfaces depends on the number of devices to be monitored, and the capabilities and limitations of the hardware.

Note: For the most up-to-date list of supported hardware platforms, network interface cards, and chipsets, see About the Hardware Compatibility Reference.

About operating system requirements

Symantec Network Security runs on Solaris 9 and Red Hat Enterprise Linux 3.0, independently of business operations. Because of this independence, Symantec Network Security can effectively secure networks that are built on any of the major operating systems, including Microsoft Windows®, Solaris, and Linux®.

Symantec Network Security is certified on the following operating systems:

- Solaris
  - Sun Solaris 9 SPARC
  - Sun Solaris 9 x86
- Linux
  - Red Hat Enterprise Linux 3.0 ES

  Note: The minimum kernel version requirements have changed between ManHunt 3.0 R1 and R2, and Symantec Network Security 4.0. Check the *Hardware Compatibility Reference* for the latest Linux kernel certified by Symantec Network Security, as well as specialized installation directions. See “About the Hardware Compatibility Reference” on page 17.

About memory requirements

The memory requirements for a Network Security software node are as follows:

- 512 MB - 1 GB RAM for Fast Ethernet configurations
- 2 GB RAM for single-Gigabit configurations
- 4 GB RAM for multi-Gigabit configurations

Note: Flow table size impacts RAM requirements. For memory requirements based on flows, see About the Hardware Compatibility Reference.

About Network Security console requirements

Install the Network Security console on a separate computer from the Symantec Network Security software node. The Network Security console is certified as follows:

- Linux
  - Red Hat Enterprise Linux 3.0 ES
- Windows
  - Microsoft Windows™ 2000/2003/XP
- Java™ 2 Runtime Environment
  - Java Runtime Environment (JRE™), standard edition 1.4.2_04
- 512 MB RAM
- Minimum screen resolution of 1024 x 768 recommended

Note: For the most up-to-date and detailed list of supported platforms and requirements, see About the Hardware Compatibility Reference.

About requirements for optional functionality

This section describes the supported platforms and requirements for SQL export and compatibility with Symantec Enterprise Security Architecture (SESA).

SQL export

Symantec Network Security supports the following SQL export options:

- MySQL version 4.0.18
- Oracle version 9i

Note: Symantec Network Security requires a dedicated computer that is separate from any other software. To export to a MySQL or Oracle database server, you must install the database software on a separate, external machine.

See “Upgrading Oracle and MySQL databases” on page 67.

SESA export

Symantec Network Security supports the following options for Symantec Enterprise Security Architecture (SESA) 2.0:

- IBM DB2 8.1
    - Windows 2000 Server
- Oracle 9*i*
    - Solaris 8 SPARC

See also “Integrating with SESA” on page 87 for more details.

Installation

This chapter includes the following topics:

- Summarizing the installation process
- Installing the Network Security software node
- Installing the Network Security console
- Uninstalling Symantec Network Security

Summarizing the installation process

This section provides a summary of the procedure for installing Symantec Network Security for the first time. Install Symantec Network Security 4.0 as follows:

To set up Symantec Network Security 4.0

1. Request the necessary licenses.
   See “Requesting license files” on page 24.
2. Gather preliminary information.
   See “Gathering preliminary information” on page 25.
3. Set up the hardware.
   See “Setting up the hardware” on page 27.
4. Attach an optional iButton, if you do not want a software token.
   See “Attaching an iButton” on page 28.
5. Set up the operating system.
   See “Setting up the operating system” on page 28.
6. Install the Symantec Network Security 4.0 software.
   See “Installing the Network Security software node” on page 30.
7. Install the Network Security console.

See “Installing the Network Security console” on page 35.

8. Perform post-installation options, such as:
   - See “Hardening the system” on page 42.
   - See “Verifying sensors” on page 46.
   - See “Adding NICs” on page 47.
   - See “Adding hardware or software tokens” on page 48.
9. Set up optional integration with additional Symantec products, such as:
   - See “Integrating with other Symantec products” on page 49.
   - See “Integrating with Smart Agents” on page 50.
   - See “Integrating with SESA” on page 51.
10. In the Network Security console, create a topology object in the Devices tab to represent the Network Security node.
    See the *Symantec Network Security Administration Guide* for instructions.

Preparing for installation

This section describes steps to take before starting installation that can make the installation procedure run more smoothly, such as requesting Symantec Network Security 4.0 licenses, gathering preliminary information, and setting up hardware and operating systems properly.

This section includes the following topics:

- Requesting license files
- Gathering preliminary information
- Setting up the hardware
- Attaching an iButton
- Setting up the operating system

Requesting license files

You must obtain a Symantec Network Security 4.0 license file for each node that you plan to install or upgrade. Each Symantec Network Security software node requires a separate license. The Network Security console does not require a license. Even if you have a license for Symantec ManHunt 3.0 R1 or R2, you must obtain a new license file for Symantec Network Security 4.0.

If the Network Security console connects to an unlicensed Network Security software node, functionality is available only to activate a license. All detection, analysis, and response capability is disabled until the license is submitted.

Caution: You must obtain a Symantec Network Security 4.0 license file for each node that you plan to install or upgrade.

See “Installing new licenses” on page 72 or “Updating licenses” on page 77.

Gathering preliminary information

Before you begin the installation process, we recommend that you gather pertinent information about master node and slave node installations.

A master node is a primary Symantec Network Security installation that ranks above all other Network Security nodes in a group or cluster. By default, the first Symantec Network Security installation is designated as the master node, and all subsequent installations within a cluster are slave nodes. Changes to a master node are propagated to the slave nodes in a cluster. Slave nodes receive updates to their topology, policies, response rules, and configuration databases from the master node.

This section includes the following topics:

- Determining IP addresses
- Determining user passphrases
- Determining node numbers
- Deciding QSP port numbers
- Using a NAT device

Determining IP addresses

Determine the IP address of each node. You must provide the same IP address that you used to install the node when you create an object to represent the node in the topology tree.

See the *Symantec Network Security Administration Guide* to find out how to populate the topology tree.

Determining user passphrases

Create strong user passphrases for connecting to the Network Security software node from the Network Security console. A strong passphrase contains at least 6 alphanumeric characters, including a combination of upper- and lower-case letters and digits, and at least one punctuation character, in random order.

See *Symantec Network Security Administration Guide*.

Determining node numbers

Determine a node number for each slave node. A master node is always assigned the node number of 1. Enter the slave node in the network topology database of the master node by creating an object in the topology tree. Make a note of the node number that you assign, using node numbers between 2- 120, inclusive.

Note: Do not attempt to change node numbers once they are assigned.

See *Symantec Network Security Administration Guide* for creating topology objects.

Deciding QSP port numbers

Determine the QSP (Query Service Provider) port number that all nodes in a cluster will share. This is the port on which the Network Security console communicates with Network Security software nodes. The port must be a valid, unused TCP port number between 1025 and 65535. Do not enter port numbers 1333, 1080, 6665-6669, 7000, and 8080. Any traffic on these ports will be analyzed by Network Security software nodes monitoring traffic.

If this is the first Network Security software node installed, then accept the default or enter any valid, unused TCP port number. All Network Security software nodes in a cluster must use the same QSP port number. Therefore, if there is an existing Network Security software node in the cluster, you must use that node’s existing QSP port number.

Verifying the QSP port number

If you are installing a slave node, verify the QSP port number using the following procedure.

To verify the QSP port number of a slave node

1. Connect to the master node from the Network Security console.
2. On the Devices tab, view the slave node in question.
   The Node Status Indicator (a red X) over the slave node indicates that it is not in sync with the master node. This can be caused by the slave node using an incorrect QSP port number. If this is the case, reinstall the slave node using the correct port number.

Note: The Node Status Indicator flags any slave nodes that are out of sync with the master node. Several circumstances can trigger this status, such as the use of an incorrect IP address, node number, QSP port number, or sync passphrase, either while installing the node, or while adding it to the topology tree.

Using a NAT device

Within the same cluster, you can position Network Security software nodes both in front of and/or behind a NAT device. All Network Security software nodes within a cluster must communicate with a given node using the same administration IP address. The administration IP address must be entered in the topology tree when adding a node object via the Network Security console.

Any node behind a NAT device must have both a local IP address and an administration IP address by which all Network Security software nodes can communicate:

- **Local IP address of the administration interface**: This is the address on the physical administration interface, which you can find by executing `ifconfig -a` on the computer.
- **Administration IP address**: This is the administration IP address that other Network Security software nodes in the cluster will use to communicate with this node. This is the same IP address used to create a node in the topology tree.

Setting up the hardware

After gathering information, set up the Network Security node by installing the hardware and software as described in this section.

Note: To optimize performance, install the Symantec Network Security software and the Network Security console on separate computers.

To set up the hardware

1. Place the Network Security node in the same physical location as routers and other network devices to be monitored. We recommend that you place the Network Security node on the same rack, whenever possible.
2. Physically connect at least one NIC on the Network Security node to each network device to be monitored.
3. Make a note of the port numbers and devices to which the interfaces are connected.

Note: If you plan to monitor a gigabit Ethernet interface, install a corresponding supported gigabit NIC.
See "About the Hardware Compatibility Reference" on page 17.

4 Connect an additional NIC to the network for communication with the Network Security console.

Attaching an iButton

The iButton is a dime-size hardware device that stores the private key portion of the Network Security signature certificate to safeguard the private key against being stolen or compromised. The iButton also performs other services, such as authentication of a Network Security node and data hashing.

If you decide to use the iButton hardware token, you must attach the iButton hardware before beginning the software installation process. If you choose not to use the hardware token, a software token will automatically be installed instead.

To install the iButton

1 Plug the iButton into its 9-pin caddy.

2 Do one of the following:

- Plug the 9-pin caddy into the appropriate serial port on the Network Security node.
- If no 9-pin serial port is available, use a DB9-DB25 adaptor.
- On systems with two serial ports available, we recommend that you use serial port 2, which is normally associated with `/dev/ttyb` on Solaris, and `/dev/cua0` on Linux.

See "Adding hardware or software tokens" on page 48 for more information about iButtons.

Setting up the operating system

After installing the hardware, set up the operating system, as described in this section.

Setting up Solaris

This section provides a summary of the Solaris installation. See the Solaris documentation for more detailed information.

To set up a Solaris operating system

1. Install the Solaris 9 operating system on your machine.
2. We recommend that you verify that the operating system was successfully installed by executing the following command:
   ```
   cat /var/sadm/system/admin/CLUSTER
   ```
   The result of this command must be as follows:
   ```
   CLUSTER=SUNWCXall
   ```
   If the result of the command differs, reinstall Solaris. Any other result indicates that the Solaris 9 installation is not in compliance with requirements.
3. We recommend that you disable `telnet` and `rlogin`, and install SSH to enable secure communication with the Network Security host.

   Note: We recommend that you use the same version of SSH on all systems.

4. Verify that all interfaces are defined, configured, and functioning correctly by executing one of the following commands:
   - To verify a specific interface, execute the following command:
     ```
     ifconfig <interface name>
     ```
   - To verify all interfaces, execute the following command:
     ```
     ifconfig -a
     ```
5. Install all security patches for Solaris from http://sunsolve.sun.com.

Setting up Red Hat Linux

This section provides a summary of the Linux installation. See the Red Hat Linux documentation for more detailed information.

To set up a Linux operating system

1. Install the Red Hat Enterprise Linux 3.0 operating system on your machine.
2. We recommend that you verify that the operating system was successfully installed, by executing the following command:
   ```
   uname -r
   ```
   Verify that the Linux kernel is version 2.4.18-14, or higher.
3. We recommend that you disable `telnet` and `rlogin`, and install SSH to enable secure communication.

   Note: We recommend that you use the same version of SSH on all systems.

4. Verify that all NICs are defined, configured, and functioning by editing the following file to enable the interface upon system startup:
   `/etc/sysconfig/network-scripts/ifcfg-<interface name>`
   See Red Hat Enterprise Linux 3.0 documentation for more information.
5. Install all security patches for Linux from http://www.redhat.com.

Installing the Network Security software node

After gathering preliminary information and installing the hardware and operating system, begin the Symantec Network Security installation process.

Take note of the following precautions:

- Install the Network Security software and Network Security console on separate computers.
- Verify that you have root privileges before starting the installation process.
- To ensure maximum performance, do not install Network Security in the root partition. See *Symantec Network Security Administration Guide*.
- Request a new Symantec Network Security 4.0 license file for each node that you plan to install.

For ease of use, this section describes the installation procedure in the following segments:

- Getting started
- Installing Symantec Network Security
- Setting up a master node
- Setting up a slave node
- Concluding the installation

Getting started

Before you begin the Network Security installation process, you must verify that the operating system is prepared.

See "Setting up the operating system" on page 28.

To prepare for installation

1. Place the CD in the CD-ROM drive, and login as root.
2. Change to the CD-ROM directory.
3. Do one of the following:

- For Red Hat Linux ES 3.0, execute the following command:
  `cd install/Linux-2.4-i86pc`
- For Solaris 9 x86, execute the following command:
  `cd install/SunOS-5.9-i86pc`
- For Solaris 9 SPARC, execute the following command:
  `cd install/SunOS-5.9-sun4u`

4 Proceed to Installing Symantec Network Security.

Installing Symantec Network Security

After completing pre-installation steps, you can start the Symantec Network Security installation procedure.

To install Symantec Network Security

1 Start the installation by executing the following command:
`./install.sh`

2 Read the End User License Agreement (EULA), and do one of the following:

- To accept the EULA, type `yes` and press **Enter**.
- To reject the EULA and abort the installation, type `no` and press **Enter**.

3 Indicate where to install Network Security by doing one of the following:

- Press **Enter** to accept the default directory `/usr/SNS`.
- Type an alternative directory and press **Enter**.

4 Verify the full host and domain name by doing one of the following:

- Press **Enter** to accept the default host name.
- Type an alternative host name and press **Enter**.

5 Read the Java license, and do one of the following:

- To accept the Java license, type `yes` and press **Enter**.
- To reject the Java license and abort the installation procedure, type `no` and press **Enter**.

6 Indicate whether to install a hardware token or a software token by doing one of the following:

- To install the iButton hardware token, type `y` and press **Enter**.
  See "About hardware tokens" on page 93.
- To install the software token, press **Enter** to accept the default `n`.
  See "About software tokens" on page 93.

7 If you selected the iButton option, indicate the path to the iButton device by choosing one of the following:

- For Solaris, press **Enter** to accept the default `/dev/ttyb` path.
- For Linux, press **Enter** to accept the default `/dev/cua0` path.
- For either, type an alternative path and press **Enter**.

The install script displays the product license information and indicates that the secure token installation is complete.

8. To indicate the qspproxy port number, do one of the following:
   - If this is the first node in a cluster, press **Enter** to accept the default port, or type any valid unused TCP port number.
   - If this is not the first node in a cluster, type the port number used in the cluster, and press **Enter**.
     See "Deciding QSP port numbers" on page 26.

   Note: If you are configuring a master node, a random QSP port will be generated for you. You can accept this default or choose your own. Take note of this port number; you need it to log into the node from the Network Security console.

9. Indicate whether or not this is the first Network Security software node installed in the cluster by choosing one of the following:
   - Type `y` if this is the first node installed in the cluster, and proceed to "Setting up a master node" on page 32.
   - Type `n`, if this is not the first node in the cluster, and proceed to "Setting up a slave node" on page 33.

Setting up a master node

If this is the first installation of Symantec Network Security, you must configure the master Network Security software node. By default, the installation procedure assigns a node number of 1 to the first Network Security software node.

To set up a master node

1. Continue from Installing Symantec Network Security.
2. Indicate whether or not the node is behind a Network Address Translation (NAT) device by choosing one of the following:
   - Press **Enter** to accept the default `n`.
     You will then be asked only to confirm the Administration IP address.
   - Type `y` and press **Enter** only if other Network Security software nodes in the cluster will address this node through a NAT.

Then, provide the Local IP address of the administration interface and the Administration IP address.
See "Using a NAT device" on page 27.

3 Enter the name of the Symantec Network Security user to add to the SuperUsers group by providing the following information:
- User name
- Passphrase
  This passphrase grants the SuperUser advanced privileges, and must be between 6 and 64 characters, inclusive.
  See "Determining user passphrases" on page 25.

4 For Solaris x86, to indicate whether gigabit interface cards are used, do one of the following:
- If no gigabit interface cards are used, type n and press **Enter**.
- If gigabit interface cards are installed, type y and press **Enter**.
  To indicate how many gigabit interface cards to start sensors on, provide an integer from 1 to 6.
  See "Verifying sensors" on page 46.

5 For Linux, do one of the following:
- Type y to perform system hardening.
- Type n to skip system hardening.

6 Wait a few minutes for the setup process to run.
When the new instance is installed, reboot the system, and proceed to "Concluding the installation" on page 34.

Setting up a slave node

After a master node has been installed, you can install up to 120 subsequent slave nodes in a cluster.

To set up a slave node

1 Continue from Installing Symantec Network Security.

2 Provide the following information about the slave Network Security software node:
- **Local node number**: This is the same node number that you must use when configuring the topology by creating a device object in the topology tree. Valid node numbers include 2-120, inclusive. Do not attempt to change node numbers after you have assigned them.

- **NAT device**: This indicates whether or not the computer is behind a Network Address Translation (NAT) device. If other Network Security software nodes in the cluster will address this node through a NAT device, then type `yes`.
- **Local IP address of the administration interface**: This is the address on the physical administration interface, which you can find by executing `ifconfig -a` on the command line.
- **Administration IP address**: This is the administration IP address that other Network Security software nodes in the cluster will use to communicate with this node. This is the same IP address used to create a node representing Network Security in the topology tree.
- **Synchronization node number**: Enter the node number of the master node with which this Network Security software node must synchronize. The master node automatically installs with a node number of 1.
- **IP address of the synchronization node**: This is the IP address of the master node with which this Network Security software node will be synchronized. Enter the correct IP address.
- **Passphrase for node 1**: Enter the synchronization passphrase, and take note so that you can provide the same passphrase when you create a device object in the topology tree.

3. For Solaris x86, to indicate whether gigabit interface cards are used, do one of the following:
   - If no gigabit interface cards are used, type `n` and proceed.
   - If gigabit interface cards are installed, type `y`.
     To indicate how many gigabit interface cards to start sensors on, provide an integer from 1 to 6.
     See “Verifying sensors” on page 46.
4. For Linux, do one of the following:
   - Type `y` to perform system hardening.
   - Type `n` to skip system hardening.
5. Wait a few minutes for the setup process to run.
   When the new instance is installed, reboot the system, and proceed to “Concluding the installation” on page 34.

Concluding the installation

This section describes the completion of the installation procedure for both master and slave node installations.

To conclude the installation procedure

1 Continue from Setting up a master node or Setting up a slave node.

2 After installing a master or slave node and rebooting, remove all media from your computer by executing the following command:

```
eject cdrom
```

3 Do one of the following:

- For Solaris, plumb the Ethernet sensor interfaces.
- For Linux, verify that all monitoring interfaces are enabled by editing the `onboot` parameter within the following file to say `yes`:

  ```
  /etc/sysconfig/network-scripts/ifcfg-<interface name>
  ```

4 Reboot the system to start the Network Security software.

5 After installation, you must configure the topology database by populating the topology tree. Symantec Network Security will not function if you do not take this step. See the *Symantec Network Security Administration Guide* for detailed instructions.

Caution: For the first several hours after a new installation starts up, Symantec Network Security aggregates statistical information about the traffic on the local network to establish a baseline of normal and expected activity. This data enables Symantec Network Security to accurately analyze whether particular incidents are attacks, and assign appropriate severity and priority levels.

6 At this point, you can perform a number of initial configuration procedures, such as adding NIC cards, converting a slave node to a master, and so on.

See “Post-installation” on page 39.

Installing the Network Security console

You can administer up to 120 nodes in a cluster using a single Network Security console, and do not need to install a separate Network Security console for each node. If you do install more than one Network Security console in a cluster, make sure to update the system configuration, topology, and response policy databases from only one console at a time. This will prevent changes made at one console from overwriting changes made at another. The Network Security console can be installed on Solaris, Linux, or Windows.

Note: To optimize performance, install the Network Security console and the Symantec Network Security software on separate computers.

Installing the Network Security console on Solaris and Linux

This section describes how to install the Network Security console on Solaris and Linux operating systems. Make sure that Java Runtime Environment (JRE) version 1.4.2_04 is installed on your computer.

To install the Network Security console on Solaris and Linux

1. Place the Symantec Network Security CD in the CD-ROM drive.
2. Login as root.
3. Change to the CD-ROM directory.
4. Change to the `install/console/unix` directory.
5. Copy the `snsadmin.jar` file to the desired `<console>` directory.
   For example:
   ```
   cp snsadmin.jar /usr/SNS_console
   ```
   See “Launching and exiting the Network Security console” on page 40.

Installing the Network Security console on Windows

This section describes how to install the Network Security console on Windows. The Windows installation of the Network Security console requires Java Runtime Environment (JRE) version 1.4.2_04.

To install the Network Security console on Windows

1. Insert the Symantec Network Security CD in the CD-ROM drive.
2. On Windows Explorer, locate the CD-ROM drive and double-click **Install** > **Windows** > **setup.exe**.
3. In **Symantec Network Security Console Setup**, click **Next**.
4. In **Welcome**, click **Next**.
5. Read the Symantec Software License Agreement, and do one of the following:
   - To accept the Agreement, type `yes` and press **Enter**.
   - To reject the Agreement and abort the installation, type `no` and press **Enter**.
6. In **Choose Destination Location**, do one of the following:
   - Click **Next** to accept the default `C:\Program Files\Symantec\SNS` directory.
   - Click **Browse** to select a different directory, and then click **Next**.
7. In **Select Components**, click **Next**.

The Network Security console and Java Runtime Environment (JRE) components are selected by default. You can deselect the JRE option if it is already installed.

8 In **Ready to Install**, click **Next**.

9 If you chose to install the JRE, follow the instructions in the JRE install dialog boxes.

10 After the installation process completes, in **Important Notes**, read the text, and click **Next**.

11 In **Finished**, click **Close**.

Establishing user accounts

The node installation process automatically creates a user account called SuperUser. After installing the Network Security console, the SuperUser can establish three additional types of user accounts: Administrator, StandardUser, and RestrictedUser accounts. The SuperUser account contains all permissions and accesses, and has the ability to establish additional pre-defined accounts with progressively fewer permissions.

Some user permissions change when upgraded from ManHunt 3.0 R1 or R2.

See the *Symantec Network Security Administration Guide* to find out how to establish additional user accounts and how permissions are allocated.

Uninstalling Symantec Network Security

This section describes how to uninstall the Symantec Network Security software and the Network Security console.

Uninstalling the Network Security software node

This section describes how to uninstall the Network Security software node.

To uninstall the Network Security software node

1 Login as root.

2 Change to the install directory by executing the following command:

```
cd <SNS_install_dir>
```

3 Execute the following command:

```
sh uninstall.sh
```

4 Do one of the following:

- Type `y` to continue the uninstall procedure.

- Type `n` to abort the uninstall procedure.

5 Remove the Symantec Network Security directory.

Note: Uninstalling the Network Security software node on either Solaris x86 or Linux automatically uninstalls the drivers.

Uninstalling the Network Security console

This section describes how to uninstall the Network Security console from a Solaris, Linux, or Windows machine.

Note: Uninstalling the Network Security console does not automatically uninstall the JRE. You can uninstall the JRE in a separate procedure.

Uninstalling on a Solaris or Linux machine

This section describes how to uninstall the Network Security console on a Solaris or Linux machine.

To uninstall the Network Security console on Solaris or Linux

◆ Delete the `snsadmin.jar` file from the console directory.

Uninstalling on a Windows machine

This section describes how to uninstall the Network Security console on a Windows machine.

To uninstall the Network Security console on Windows

1 Click **Start** > **Programs > Symantec Network Security**.

2 Click **Remove Symantec Network Security**.

Chapter 4

Post-installation

This chapter includes the following topics:

- About post-installation procedures
- Hardening the system
- Managing gigabit drivers
- Verifying sensors
- Adding NICs
- Adding hardware or software tokens
- Setting up SQL export
- Integrating with other Symantec products

About post-installation procedures

After installation, you can enhance your system by hardening it, or adding drivers, NICs, or tokens. You can also perform post-installation setup, such as establishing failover groups or integrating with other products such as SESA, Smart Agents, and DeepSight.

This section describes basic starting and stopping procedures integral to any post-installation procedure:

- Launching and exiting the Network Security console
- Restarting and rebooting Network Security software nodes

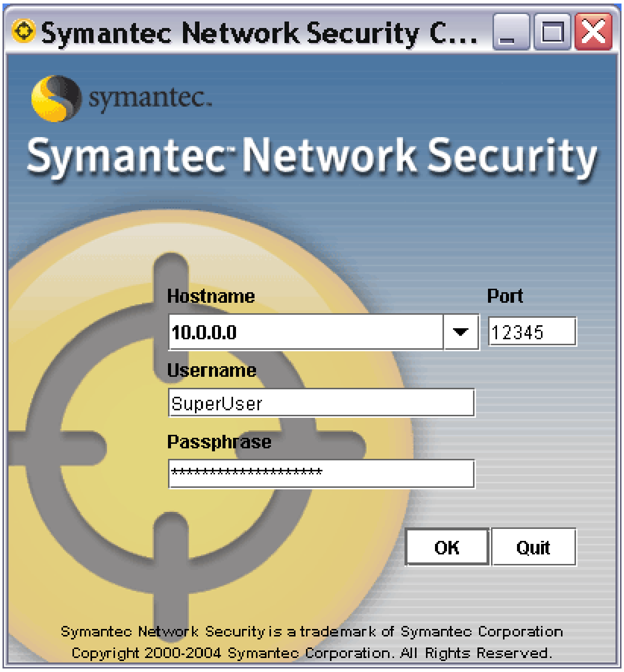
Launching and exiting the Network Security console

This section describes how to start and stop the Network Security console. This section includes the following topics:

- Launching the Network Security console
- Exiting the Network Security console

Launching the Network Security console

This section describes how to launch the Network Security console on Windows, Solaris, and Linux.



Hostname
10.0.0.0

Port
12345

Username
SuperUser

Passphrase
****

Symantec Network Security is a trademark of Symantec Corporation
Copyright 2000-2004 Symantec Corporation. All Rights Reserved.

To launch the Network Security console

1 Depending on the operating system, do one of the following:

- For Windows, double-click the Symantec Network Security icon on the desktop.
- For Solaris or Linux, run the following command:

  ```
  <path to java>/bin/java -Xmx256M -jar snsadmin.jar
  ```

  For example:

  ```
  /usr/SNS/java/jre/bin/java -Xmx256M -jar snsadmin.jar
  ```

Note: The Network Security console requires Java 1.4.2_04 to run.

2. In **Hostname**, enter the hostname or IP address of the software or appliance node to monitor.
3. In **Port**, enter the port number. If in a cluster, all nodes must use the same port number.
4. In **Username**, enter the user name. Access and permissions depend on the user group of your login account.
5. In **Passphrase**, enter the passphrase established for your user login account, and click **OK**.

Exiting the Network Security console

All users can exit the Network Security console on Windows, Solaris, and Linux.

To stop the Network Security console

◆ On Solaris, Linux, or Windows, simply click **File** > **Exit**.

Restarting and rebooting Network Security software nodes

This section describes how to restart and reboot Network Security software nodes from the Network Security console, and how to start and stop Network Security software nodes from the command line. This section includes the following topics:

- Restarting from the Network Security console
- Rebooting from the Network Security console
- Starting and stopping nodes manually

Restarting from the Network Security console

This section describes how to restart the Network Security software node from the Network Security console.

To restart the Network Security software node

1. In the Network Security console, click **Admin > Node > Restart Network Security Application**.
2. Select the Network Security software node that you want to restart from the pull-down list, and click **OK**.

3. Wait until the Network Security console display indicates that the restart process has completed.

Rebooting from the Network Security console

This section describes how to reboot the Network Security software node from the Network Security console.

To reboot the Network Security software node

1. In the Network Security console, click **Admin > Node > Reboot Network Security Node**.
2. Select the Network Security software node that you want to reboot from the pull-down list, and click **OK**.
3. Wait until the Network Security console display indicates that the reboot process has completed.

Starting and stopping nodes manually

This section describes how to start and stop the Network Security software node from the command line.

To stop, start, or restart Network Security manually

- To manually stop Network Security, execute the following command:
  `<SNS_install_dir>/stop`
- To manually start Network Security, execute the following command:
  `<SNS_install_dir>/start`
- To manually restart Network Security, execute the following command:
  `<SNS_install_dir>/restart`

Hardening the system

This section describes how to enhance your Solaris system by hardening. You can harden a Linux system during the installation process. This section includes the following topics:

- Hardening Solaris systems
- Hardening Linux systems

Hardening Solaris systems

We recommend you use the Solaris Security Toolkit, also known as JASS v. 4.0.2, to minimize, harden, and secure your Solaris operating system. See http://wwws.sun.com/software/security/jass/ for more information about the JASS toolkit.

When Network Security is installed, the following Solaris services are automatically disabled in runlevels 2 and 3 to improve security:

- `70uucp`
- `71ldap.client`
- `72slpd`
- `73cachefs.daemon`
- `76snmpdx`
- `80lp`
- `88sendmail`
- `96ab2mgr`

Thus, UUCP, LDAP, service location, `cachefs`, SNMP, printing, sendmail, and the answer book manager are all disabled on the Network Security software node.

Hardening Linux systems

You can harden a Linux system during the installation process. The installation script includes an option to harden the Linux system.

Managing gigabit drivers

The Symantec Network Security gigabit driver enhances gigabit monitoring if you are using the gigabit cards supported by Network Security. For speeds greater than 600 Mb/s, you need a Symantec Network Security gigabit driver.

Note: Symantec Network Security does not support gigabit drivers on Solaris SPARC. The Symantec Network Security gigabit driver can utilize from 1 to 6 Intel PRO/1000 NICs currently. The NIC interfaces are not visible in `ifconfig`. See “About node requirements” on page 19.

This section includes the following topics:

- Loading gigabit drivers
- Verifying gigabit drivers on Solaris

- Verifying gigabit drivers on Linux
- Uninstalling Symantec Network Security gigabit drivers

Loading gigabit drivers

This section describes how to install the Symantec Network Security gigabit driver on a Solaris machine after the Symantec Network Security installation. The Symantec Network Security gigabit driver enables you to monitor from 1 to 6 gigabit interfaces when running Network Security on a Solaris x86 computer.

Installation of the Symantec Network Security gigabit driver can be done during the Network Security installation process. The installation script asks if you have gigabit NICs to monitor. If you indicated that you did, the script installed the Symantec Network Security gigabit driver. If you indicated that you did not, you can install a gigabit driver separately.

To install a Symantec Network Security gigabit driver

1. Uninstall the existing Intel driver.
   See the Solaris Intel documentation for instructions. This process may require that you reboot the node.
2. Install the Symantec Network Security gigabit driver on each gigabit card by executing the following from the `<SNS_install_dir>` directory:
   `./re1000-install.sh`
3. Type the number of gigabit interfaces to monitor, and press **Enter**.
   The driver enables you to monitor from 1 to 6 gigabit interfaces.
4. Restart the machine.
5. Launch the Network Security console and edit the interface name for each interface in the topology tree to match the interface naming convention used by the new driver.
   For example, `eth0`, `hme0`, or `iprb0` must be renamed to `re1000g0`.
   See the *Symantec Network Security Administration Guide* for more detailed instructions about editing monitoring interfaces in the topology tree.

Verifying gigabit drivers on Solaris

The Symantec Network Security gigabit driver now enables you to monitor from 1 to 6 gigabit interfaces with one sensor per gigabit when running Symantec Network Security on a Solaris machine.

The Symantec Network Security gigabit driver on Solaris installs as a part of the Symantec Network Security installation. The following step enables you to verify that the driver was added during installation.

Note: Always load drivers using `mhdrv-ctl`, not by hand.

To verify that the NIC interface was installed on Solaris

1. Reboot the Solaris machine.
2. Execute the following command:
   ```
   <SNS_install_dir>/tools/mhdrv-ctl status
   ```
   This command will list interfaces monitored by Symantec drivers. See *Symantec Network Security Administration Guide* for more information about interfaces.

Verifying gigabit drivers on Linux

The Symantec Network Security gigabit driver on Linux installs as a part of the Symantec Network Security installation. The following step enables you to verify that the driver was added during installation.

To verify that the NIC interface was installed on Linux

1. Reboot the Linux machine.
2. Execute the following command:
   ```
   mhdrv-ctl status
   ```
   This command will list interfaces monitored by Symantec drivers. See *Symantec Network Security Administration Guide* for more information about interfaces.

Note: The Symantec Network Security gigabit driver on Linux installs as a part of the Symantec Network Security installation. You cannot add gigabit drivers manually after installation. In Linux, the driver cannot specify NIC arguments.

Uninstalling Symantec Network Security gigabit drivers

Device drivers are software that control a hardware component. Stock drivers come with the operating system, and Symantec Network Security provides custom drivers as well.

For all platforms, the drivers are uninstalled as part of the uninstallation of the Symantec Network Security software. For Solaris x86, you have the option of uninstalling the Symantec Network Security gigabit drivers separately.

To uninstall a Symantec Network Security gigabit driver

1. Stop Symantec Network Security by executing the following command:

   ```
   <SNS_install_dir>/stop
   ```

2. Run the uninstall script by executing the following command:

   ```
   <SNS_install_dir>/re1000-uninstall.sh
   ```

3. Reboot the machine.

4. Reinstall the Intel PRO/1000 stock driver.

   Note: Make sure that the name of each monitoring interface matches the interface naming convention used by the Intel driver, such as `e1000g0`, `e1000g1`, and so on. See the *Symantec Network Security Administration Guide* for detailed instructions.

Verifying sensors

This section describes how to verify that sensors are running on Fast Ethernet drivers on Solaris and Linux computers.

This section includes the following topics:

- Running sensors on Solaris
- Running sensors on Linux

See “About the Hardware Compatibility Reference” on page 17 for the most up-to-date list of supported drivers, gigabit NICs, and chipsets.

Running sensors on Solaris

If you are running Solaris stock drivers, verify that the sensor interfaces are plumbed before you start Symantec Network Security to make sure that the sensors can detect traffic. This cannot be done if you have installed the Symantec Network Security gigabit driver.

To run sensors on Solaris

1. To verify that the sensor interface has been plumbed, execute the following command:

   ```
   /usr/sbin/ifconfig -a
   ```

2. If the interface has been plumbed, review the response. It should be similar to the following:

   ```
   iprb1: flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
   index 3
   inet 0.0.0.0 netmask 0
   ```

```
ether 0:3:47:72:f4:a5
```

3. If the interface has not been plumbed, add an empty hostname file corresponding to the interface.

   For example, to add a hostname file for the interface qfe2, execute the following commands:

   ```
   touch /etc/hostname.qfe2
   ```

Running sensors on Linux

Verify that all interfaces are enabled and running during boot time. It is essential to perform these steps in the correct order.

To run sensors on Linux

◆ Verify that all monitoring interfaces are up and running (the equivalent of plumbing the interfaces on Solaris) by completing the following steps:

- Edit the following file:

  ```
  /etc/sysconfig/network-scripts/ifcfg-<interface name>
  ```

- In the `<interface name>` file, edit the `onboot` parameter to say `yes`.
- Reboot the Linux computer.

Adding NICs

After backup and restore upgrades, check that the physical interface names on the restore machine are the same as those on the backed up system. If the names differ, you must edit each monitoring interface in the topology tree, and set the correct interface name. After in-place upgrades, you do not need to make any changes to the NICs.

This section describes how to add gigabit NICs to Symantec Network Security on Solaris and Linux machines.

See "About the Hardware Compatibility Reference" on page 17 for the most up-to-date list of supported NICs and chipsets.

Adding NICs on Solaris

This section describes how to add gigabit NICs on Solaris x86 machines.

To add a gigabit NIC on Solaris

1. Physically install the NIC in the Solaris machine.
2. Execute the following command:

   ```
   vi /kernel/drv/re1000.conf
   ```

3 Change the number of interfaces from the default value of 2, to a value between 1-6, by editing the following line:

```
num-gb-interfaces= <1-6>
```

4 Perform a reconfiguration reboot by executing the following command:

```
touch /reconfigure
reboot
```

Adding NICs on Linux

This section describes how to add gigabit NICs on Linux machines.

To add a gigabit NIC on Linux

1 Physically install the NIC in the Linux machine.

2 Reboot by executing the following command:

```
reboot
```

Adding hardware or software tokens

Symantec Network Security provides two types of tokens used to sign log files: the software token and the hardware token (also called the iButton™). During installation, you can choose either an iButton or a software token. At any time after installation, you can change that setting.

During the upgrade procedure, if you used an iButton in the previous installation, you can choose to continue or to switch to a software token. If you used a software token in the previous installation, the upgrade procedure will default to continue using a software token.

Both software tokens and iButtons can be installed during the installation process. After Symantec Network Security is up and running, you can use the `<SNS_install_dir>/token-intall.sh` and `token-remove.sh` scripts to switch.

See "Using iButtons" on page 93 to find out how to install, remove, and manage software and iButton tokens.

Setting up SQL export

To export to Oracle 9*i* or MySQL 4.0, you must establish export tables for the incident and event databases, obtain appropriate database drivers from a vendor and add them manually, and configure the SQL Export parameters. Although the export tables reside on the software node, the database server must reside on a separate computer.

To set up SQL export

1. Establish export tables for the incident and event databases, referencing the following files provided by Symantec Network Security:
   - For the Oracle database, use the following:
     `/usr/SNS/dbs/oracle-sqltable.statements`
   - For the MySQL database, use the following:
     `/usr/SNS/dbs/mysql-sqltable.statements`
2. Obtain a supported database driver from the vendor, rename, and save as follows:
   - For the Oracle driver, use the following:
     `<sns_install_dir>/java/jdbcdriver-oracle-9i.jar`
   - For the MySQL driver, use the following:
     `<sns_install_dir>/java/jdbcdriver-mm.mysql.2.0.14.jar`
3. Restart Symantec Network Security.
4. Configure the SQL Export parameters.
   See the *Symantec Network Security Administration Guide* to find out how to configure the SQL Export parameters.

Note: Symantec Network Security requires a dedicated computer that is separate from any other software. To export to a MySQL or Oracle database server, you must install the database software on a separate, external machine.

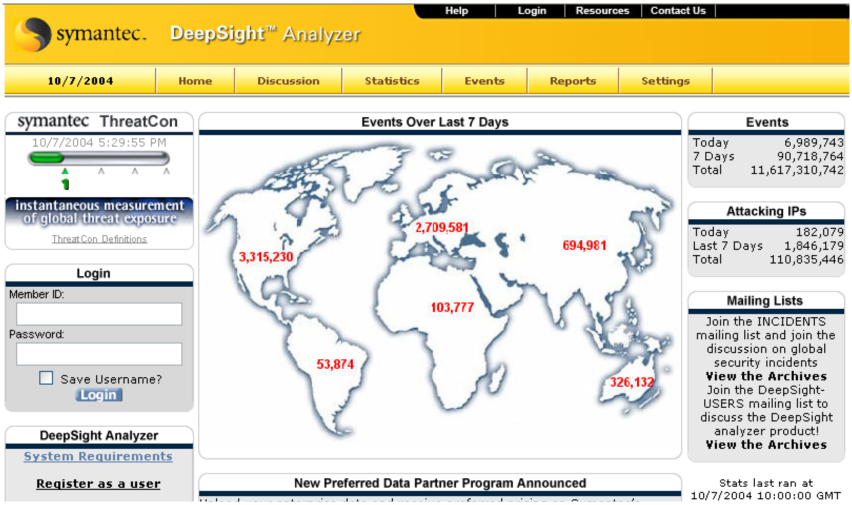
Integrating with other Symantec products

This section includes the following topics:

- Integrating with DeepSight
- Integrating with Smart Agents
- Integrating with SESA

Integrating with DeepSight

Symantec DeepSight™ provides customized and comprehensive alerts of cyber attacks worldwide, with countermeasures to prevent attacks before they occur, enabling companies to mitigate risk, manage threats, and ensure business continuity.



Events

Today	6,989,743
7 Days	90,718,764
Total	11,617,310,742

Attacking IPs

Today	182,079
Last 7 Days	1,846,179
Total	110,835,446

Mailing Lists

Join the INCIDENTS mailing list and join the discussion on global security incidents
View the Archives
Join the DeepSight-USERS mailing list to discuss the DeepSight analyzer product!
View the Archives

Stats last ran at 10/7/2004 10:00:00 GMT

Your security events are automatically submitted to Symantec by a software program called DeepSight Extractor. Once submitted, your security events join those of thousands of other individuals, and allow Symantec to see widespread attack activity on the Internet.

To get started quickly, see the DeepSight documentation on the Symantec Network Security installation CD, in the `root/.extractor` directory, or on the documentation Web site.

To view DeepSight documentation

1. Open the following URL:
   www.symantec.com/techsupp/enterprise/select_product_manuals.html
2. Click **Early Warning Solutions** > **Symantec DeepSight**.

Integrating with Smart Agents

The Symantec Network Security management system can be used to expand the intrusion protection umbrella using the Symantec Network Security Smart Agents (Smart Agents) to provide enterprise-wide, multi-source intrusion management by aggregating, correlating, and responding to events from multiple Symantec and third-party host and network security products.

Symantec Network Security Smart Agents enable enterprise-wide, multi-source intrusion event collection, helping companies to expand the security umbrella and enhance the threat detection value of their existing security assets. Third-party intrusion events are aggregated into a centralized location, leveraging the power of the Symantec Network Security correlation and analysis framework, along with the ability to automate responses to intrusions across the enterprise.

The following Smart Agents will be upgraded to be compatible with Symantec Network Security 4.0:

- Symantec Network Security Smart Agent for Snort 2.0
- Symantec Network Security Smart Agent for Cisco IDS 4.0
- Symantec Network Security Smart Agent for Dragon 6.0

To view Symantec Network Security Smart Agent documentation

1. Open the following URL:
   www.symantec.com/techsupp/enterprise/products/manhunt/manhunt_sa/manuals.html
2. Click **Intrusion Protection** > **Symantec Network Security 4.0** > **Symantec Network Security Smart Agents**.

Integrating with SESA

Symantec Network Security can integrate with SESA through the SESA Bridge. The Symantec Network Security SESA™ Bridge allows you to send events from Symantec Network Security™ 4.0 to the Symantec Enterprise Security Architecture (SESA) 2.0 Management Console.

To find out more about SESA and how to integrate with it, see “Integrating with SESA” on page 87.

Upgrading

This chapter includes the following topics:

About upgrading

The following topics are worthy of consideration before starting an upgrade:

- Upgrading from ManHunt 3.0 and earlier
- Upgrading from ManHunt 3.0 R1 and later
- Choosing an upgrade strategy

Upgrading from ManHunt 3.0 and earlier

Upgrading from ManHunt 3.0 directly to Symantec Network Security 4.0 is not supported. To upgrade from an existing ManHunt 3.0 installation or earlier, you must first upgrade to ManHunt 3.0 R1 (3.0.1). Then follow the in-place upgrade procedure for Symantec Network Security 4.0. Make sure that you also upgrade to the supported platform, operating system, distribution, and patch set before installing Symantec Network Security 4.0.

See “About the Hardware Compatibility Reference” on page 17 for detailed information about supported platforms and operating systems.

Upgrading from ManHunt 3.0 R1 and later

You can upgrade from ManHunt 3.0 R1 or R2 using the automatic in-place install script. You must obtain a Symantec Network Security 4.0 license file for each node that you plan to install or upgrade. The upgrade does not require a new certificate and iButton, nor does it require an update to the topology or response rule databases. Make sure that you also establish the recommended operating system version, distribution, and patch set before upgrading to Symantec Network Security 4.0.

See “About node requirements” on page 19.

See “Upgrading licenses” on page 65.

See “Running an in-place upgrade” on page 57.

Choosing an upgrade strategy

Symantec Network Security supports the following two upgrade strategies:

- In-place upgrade: A seamless process that brings a ManHunt 3.0 R1 (3.0.1) or R2 installation up to Symantec Network Security 4.0, preserves the existing configuration, and produces HTML reports that log the components that were affected. Use this strategy if you are upgrading from ManHunt 3.0 R1 (3.0.1) or R2 on a supported hardware and operating system combination that you do not plan to change.
- Backup and restore upgrade: An alternative strategy that backs up the existing configuration, enables you to upgrade or migrate to new operating systems or hardware platforms, installs Symantec Network Security 4.0, and then restores the ManHunt 3.0 R1 or R2 configuration. Use this strategy if you are upgrading from ManHunt 3.0 R1 (3.0.1) or R2 on a hardware platform and/or operating system that is no longer supported.

Upgrade strategies for ManHunt 3.0 R1 or R2

Depending on whether you want to upgrade your operating system, platform, and other components, as well as your ManHunt 3.0 R1 or R2 installation, you can choose between the in-place upgrade and the backup and restore upgrade strategies.

The following table lists the available upgrade strategies for ManHunt 3.0 R1 or R2:

Table 5-1 Valid upgrade strategies for specific situations

Hardware platform	Operating system	Operating system	Type of upgrade
From ManHunt 3.0 R1 or R2		**To Symantec Network Security 4.0**	
Sun V60x	From Solaris 9 x86	To Solaris 9 x86	Running an in-place upgrade
Dell 6650	From Red Hat Enterprise Linux 3.0	To Red Hat Enterprise Linux 3.0	Running an in-place upgrade
Sun Fire V210	From Solaris 8 SPARC	To Solaris 9 SPARC	Running a backup/restore upgrade
Sun Fire V240	From Solaris 8 SPARC	To Solaris 9 SPARC	Running a backup/restore upgrade
Dell 1750	From Red Hat Linux 8	To Red Hat Enterprise Linux 3.0	Running a backup/restore upgrade
Dell 2650	From Red Hat Linux 8	To Red Hat Enterprise Linux 3.0	Running a backup/restore upgrade
Dell 2650	From Solaris 8 x86	To Red Hat Enterprise Linux 3.0	Running a backup/restore upgrade
HP / Compaq Proliant DL380G3	From Red Hat Linux 8	To Red Hat Enterprise Linux 3.0	Running a backup/restore upgrade
HP / Compaq Proliant DL380G3	From Solaris 8 x86	To Red Hat Enterprise Linux 3.0	Running a backup/restore upgrade
HP / Compaq Proliant DL580G2	From Red Hat Linux 8	To Red Hat Enterprise Linux 3.0	Running a backup/restore upgrade

Note: See “About the Hardware Compatibility Reference” on page 17 for the latest information about supported hardware platforms and operating systems.

Upgrade strategies for iForce

The following table illustrates the available upgrade strategies for iForce:

Table 5-2 Valid upgrade strategies for iForce

Hardware platform	Operating system	Operating system	Type of upgrade
ManHunt 3.0 R1/R2 on iForce 2.0		**To Symantec Network Security 4.0**	
Sun LX50	From iForce 2.0 with ManHunt 3.0 R1 or R2	To iForce 2.0 with Symantec Network Security 4.0	Upgrading iForce
Sun V60x	From Solaris 9 x86 iForce 2.0 with ManHunt 3.0 R1 or R2	To iForce 2.0 with Symantec Network Security 4.0	Upgrading iForce

Upgrade strategies for ManHunt 3.0

The following table illustrates the only upgrade strategy for ManHunt 3.0:

Table 5-3 Valid upgrade strategy for ManHunt 3.0

Hardware platform	Operating system	Operating system	Type of upgrade
From ManHunt 3.0		**To Symantec Network Security 4.0**	
From any hardware	From any operating system	To any operating system	Upgrade to ManHunt 3.0 R1, then see Running a backup/restore upgrade

Ensuring free space

The backup script checks to see if the system has enough free space on the root disk partition to store the backup of the ManHunt 3.0 R1 or R2 configuration. If an error message indicates that there is not enough free space, you can free up some space by moving archived logs from the `<SNS_install_dir>/oldlogs` directory to another machine or another disk partition.

Running an in-place upgrade

Symantec Network Security 4.0 supports upgrading directly from ManHunt 3.0 R1 or R2 without having to restore the ManHunt configurations.

This section includes the following topics:

- Preparing for an in-place upgrade
- Upgrading in-place
- After an in-place upgrade

Preparing for an in-place upgrade

Before starting the upgrade process, we recommend that you consider the following:

- Obtain a new Symantec Network Security 4.0 license file for each node that you plan to upgrade.
  See "About Symantec licenses" on page 71.
- Make sure that you have certified hardware and platforms.
  See "About node requirements" on page 19.
- Obtain root privileges.
- Verify that you have enough disk space to store the backup configuration.
  See "Ensuring free space" on page 56.

Upgrading in-place

This section describes how to upgrade a Network Security software node from ManHunt 3.0 R1 or R2 to Symantec Network Security 4.0 using the in-place procedure.

To upgrade a Network Security software node

1. Place the CD in the CD-ROM drive.
2. Login as root.
3. Change to the CD-ROM directory, where you can view the following directories:
   - Red Hat Linux ES 3.0:
     `install/Linux-2.4-i86pc`
   - Solaris 8 x86:
     `install/SunOS-5.8-i86pc`
   - Solaris 9 x86:

```
install/SunOS-5.9-i86pc
```

- Solaris 9 SPARC:

  ```
  install/SunOS-5.9-sun4u
  ```

4 Change to the upgrade directory by executing the following command:

```
cd /<CD drive>/install/<platform>/upgrade/
```

5 Start the upgrade procedure by executing the following command:

```
sh upgrade.sh
```

6 To confirm that you have updated license files, do one of the following:

- Type `y` and press **Enter** to continue the procedure.
- Type `n` and press **Enter** to abort the procedure.

  See “About Symantec licenses” on page 71.

7 Wait while the script stops processes, backs up the ManHunt installation, and archives databases. Depending upon the size of the databases, this process can take several minutes.

8 To confirm that you agree to have ManHunt uninstalled, do one of the following:

- Type `y` and press **Enter** to indicate that you want to proceed.
- Type `n` and press **Enter** to abort the procedure.

9 To indicate whether you are upgrading a master node, do one of the following:

- Type `y` and press **Enter** to indicate that this is a master node.
- Type `n` and press **Enter** to indicate that this is a slave node.

10 Wait while the script extracts the product, creates scripts, installs policies and LiveUpdate packages, and indicates that the upgrade was successful.

11 Note the location of the upgrade report and upgrade log files.

The following example shows the locations of the report file and report log:

- Report at `/SNS_install_dir/upgrade/upgrade_report.html`
- Log at `/SNS_install_dir/upgrade/upgrade.<logfile_number>.log`

  See “Verifying success via the report log” on page 59.

12 After the process has finished, remove all media from your machine.

13 Reboot the node machine using one of the following commands:

- `init 6` (recommended)
- `reboot`

14 Do one or both of the following:

- To upgrade the Network Security console, see “Upgrading the Network Security console” on page 65.

- To add new licenses, see "About Symantec licenses" on page 71.

After an in-place upgrade

After completing the upgrade procedure, you can perform the following:

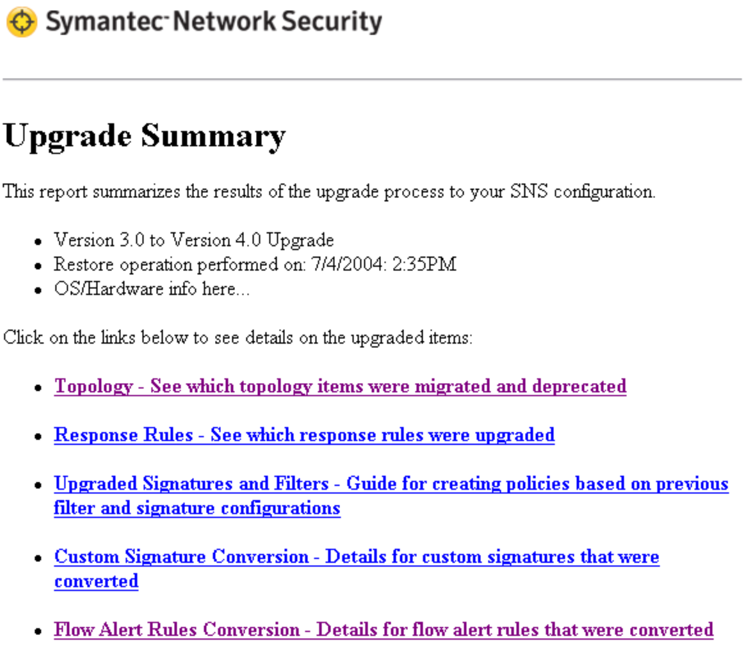
- Verifying success via the report log
- Converting old log files

Verifying success via the report log

The upgrade process produces HTML reports that specify which areas were upgraded, such as signatures, flow alert rules, policies, and response rules. Each report lists the total number of files, successful migrations, and files that failed to migrate. They are packaged in a single tar file that you can transfer to another machine for easy viewing, such as a client that has a browser. The files are located in the following directory:

```
<SNS_install_dir>/upgrade/
```

The upgrade process summarizes the upgrade, such as the following example:



Symantec Network Security

Upgrade Summary

This report summarizes the results of the upgrade process to your SNS configuration.

- Version 3.0 to Version 4.0 Upgrade
- Restore operation performed on: 7/4/2004: 2:35PM
- OS/Hardware info here...

Click on the links below to see details on the upgraded items:

- **Topology - See which topology items were migrated and deprecated**
- **Response Rules - See which response rules were upgraded**
- **Upgraded Signatures and Filters - Guide for creating policies based on previous filter and signature configurations**
- **Custom Signature Conversion - Details for custom signatures that were converted**
- **Flow Alert Rules Conversion - Details for flow alert rules that were converted**

Converting old log files

After upgrading from ManHunt 3.0 R1 or R2 to 4.0, you can use the `convertlogs_mh3.sh` script to manually convert old log files from your 3.0 R1 or R2 configuration to the new 4.0 format. The upgrade process does not convert all old log files, which enables you to selectively upgrade the log files. You can find the script in the following location:

```
<SNS_install_dir>/tools/convertlogs_mh3.sh
```

To convert old log files

1. Login as root.
2. Execute the following command:

   ```
   <SNS_install_dir>/tools/convertlogs_mh3.sh <filename of log to
   convert>
   ```

To view converted log files

1. In the Network Security console, click **Admin** > **Node** > **Manage Logs**.
2. Select the node.
3. Click the archived log that you want to view.

Note: After the upgrade procedure, you can also upgrade system components. See “Upgrading components” on page 65.

Running a backup/restore upgrade

Symantec Network Security 4.0 supports a second method of upgrading by backing up and restoring the ManHunt 3.0 R1 or R2 configuration. This enables you to preserve the existing configuration while migrating to a new operating system, new platform, or new host machine.

This section describes the following:

- Preparing for backup/restore upgrade
- Upgrading via backup/restore

Preparing for backup/restore upgrade

Before starting the upgrade process, we recommend that you consider the following:

- Obtain a new Symantec Network Security 4.0 license file for each node that you plan to upgrade.
  See "About Symantec licenses" on page 71.
- Make sure that you have certified hardware and platforms.
  See "About node requirements" on page 19.
- Obtain root privileges.
- Verify that you have enough disk space to store the backup configuration.
  See "Ensuring free space" on page 56.
  See "Creating an optional log file" on page 64.
- Preserve the original IP address of the node to use the same address after the upgrade as before. The backup/restore upgrade strategy restores the ManHunt 3.0 R1 or R2 configuration, including IP addresses. If these change, Symantec Network Security will not function properly.

Upgrading via backup/restore

This section describes how to follow the backup/restore procedure to upgrade a Network Security software node from ManHunt 3.0 R1 or R2. If you are upgrading to a new machine, or upgrading the operating system or platform of the same machine, use the backup/restore procedure. You can complete this procedure in three basic steps:

- Backing up the ManHunt configuration
- Upgrading to a new hardware platform
- Migrating to a new operating system
- Restoring the ManHunt 3.0 R1 or R2 configuration

Backing up the ManHunt configuration

This section describes how to back up the ManHunt 3.0 R1 or R2 configuration before migrating to a new machine, operating system, or hardware platform.

In addition to upgrading on the same hardware or operating system, you can upgrade the operating system or move to a new system. Below are all the supported operating system migrations from ManHunt 3.0 R1 or R2 to Symantec Network Security 4.0:

- Solaris 8 SPARC -> Solaris 9 SPARC

- Solaris 8 Intel Edition -> Solaris 9 Intel Edition
- Solaris 8 Intel Edition -> Red Hat ES 3
- Solaris 9 Intel Edition -> Red Hat ES 3
- Red Hat ES 3 -> Solaris 9 Intel Edition
- Red Hat 8.0 -> Red Hat ES 3
- Red Hat 8.0 -> Solaris 9 Intel Edition

To back up a ManHunt 3.0 R1 or R2 configuration

1. Place the CD in the CD-ROM drive.
2. Login as root.
3. Change to the CD-ROM directory.
4. From the CD-ROM directory, do one of the following:
   - For Red Hat Linux ES 3.0, execute the following command:

     ```
     cd install/Linux-2.4-i86pc
     ```
   - For Solaris 9 x86, execute the following command:

     ```
     cd install/SunOS-5.9-i86pc
     ```
   - For Solaris 9 SPARC, execute the following command:

     ```
     cd install/SunOS-5.9-sun4u
     ```
5. Change to the upgrade directory by executing the following command:

   ```
   cd /<CD drive>/install/<platform>/upgrade/
   ```
6. Stop ManHunt 3.0 R1 or R2 processes.
7. Execute the following command:

   ```
   sh backup_mh3.sh <name of backup file>
   ```

   If you do not supply the optional `<name of backup file>` filename, the progress data appears temporarily on your terminal screen, but is not saved.
8. By default, the backup file is created in a `tmp/mhupgrade` directory. Move the backup file to a safe location on another machine using a program such as SCP or FTP, execute the following command:

   ```
   scp <filename> <path to new location>
   ```
9. To continue, do one of the following:
   - If you are upgrading on a new machine, or upgrading the hardware platform of the original machine, proceed to "Upgrading to a new hardware platform" on page 63.
   - If you are upgrading on a new operating system, proceed to "Migrating to a new operating system" on page 63.

Upgrading to a new hardware platform

If you are running a backup/restore upgrade on a new machine, or upgrading the operating system or platform of the same machine, use this procedure.

To migrate from one hardware platform to another

1. Verify that the existing ManHunt 3.0 R1 or R2 configuration files are successfully backed up.
2. Install the new machine.
3. Proceed to "Restoring the ManHunt 3.0 R1 or R2 configuration" on page 63 to install Symantec Network Security 4.0 using the install script with a restore argument.

Migrating to a new operating system

This section describes how to migrate from ManHunt 3.0 R1 or R2 on one operating system to Symantec Network Security 4.0 on a new operating system.

To migrate from one operating system to another

1. Verify that the existing ManHunt 3.0 R1 or R2 configuration files are successfully backed up.
2. Install the new operating system.
3. Proceed to "Restoring the ManHunt 3.0 R1 or R2 configuration" on page 63 to install Symantec Network Security 4.0 using the install script with a restore argument.

Restoring the ManHunt 3.0 R1 or R2 configuration

If you are running a backup/restore upgrade on a new machine, or upgrading the operating system or platform of an old machine, use this procedure to restore the ManHunt 3.0 R1 or R2 configuration in the Symantec Network Security system.

To install Symantec Network Security with the ManHunt 3.0 R1 or R2 configuration

1. Change to the Symantec Network Security 4.0 upgrade directory by executing the following command:

   ```
   cd /<CD drive>/install/<platform>/upgrade/
   ```

2. Start the installation procedure with a restore argument by executing the following command:

   ```
   sh install.sh -restore <path to backup logfile>
   ```

For example:

```
sh install.sh -restore /tmp/mhupgrade/<timestamped filename>
```

3 To confirm that you have updated license files, do one of the following:

- Type `y` and press **Enter** to indicate that you have updated license files.
- Type `n` and press **Enter** to abort the procedure.
  See "About Symantec licenses" on page 71.

4 To indicate whether you are upgrading a master node, do one of the following:

- Type `y` and press **Enter** to indicate that this is a master node.
- Type `n` and press **Enter** to indicate that this is a slave node.

5 Wait while the script extracts the product, creates scripts, restores the ManHunt configuration, and indicates that the upgrade was successful.

6 Note the location of the upgrade report and upgrade log files. For example:

- Report at `/usr/manhunt/upgrade/upgrade_report.html`
- Log at `/usr/manhunt/upgrade/upgrade.123456789123.log`
  See "Verifying success via the report log" on page 59.

7 After the process has finished, remove all media from your machine.

8 Reboot the machine using one of the following commands:

- `init 6` (recommended)
- `reboot`

After upgrading via backup/restore

You can perform the following optional tasks after the upgrade procedure is complete:

- Creating an optional log file
- Verifying success via the report log

Creating an optional log file

The `backup_mh3.sh` and `install.sh` files include an optional parameter for creating a log file. If you supply a log filename when running these two scripts, the progress information will be saved to the file. This is useful if you want to archive the backup log file or transfer it to another location, such as during a backup/restore upgrade. If you choose not to supply the optional log filename when running these two scripts, the progress information will appear temporarily on your terminal screen, but will not be saved to a file.

Verifying success via the report log

The upgrade process produces HTML reports that specify which areas were upgraded, such as signatures, flow alert rules, policies, and response rules. Each report lists the total number of files, successful migrations, and files that failed to migrate. They are packaged in a single tar file that you can transfer to another machine for easy viewing, such as a client that has a browser.

Note: After the upgrade procedure, you can also upgrade system components.

See "Upgrading components" on page 65.

Upgrading the Network Security console

To upgrade the ManHunt console to Symantec Network Security 4.0, install a new Symantec Network Security 4.0 console.

See "Installing the Network Security console" on page 35.

Upgrading components

This section describes the upgrade issues to consider when upgrading components of Symantec Network Security, such as licenses, databases, drivers, tokens, and signatures.

This section includes the following topics:

- Upgrading licenses
- Upgrading a node behind a NAT device
- Upgrading NIC cards
- Upgrading tokens
- Upgrading signatures
- Upgrading Oracle and MySQL databases
- Upgrading SESA Agents

Upgrading licenses

Existing licenses are not upgraded. Each Symantec Network Security software node requires a separate, current license. The Network Security console does not require a license. You must obtain a Symantec Network Security 4.0 license file for each node that you plan to install or upgrade.

If the Network Security console connects to an unlicensed Network Security software node, functionality is available only to activate a license. All detection, analysis, and response capability is disabled until the license is submitted.

Caution: You must a Symantec Network Security 4.0 license file for each node that you plan to upgrade, before beginning either the in-place upgrade or the backup/restore process.

See “Updating licenses” on page 77.

Upgrading NIC cards

This section describes how to physically change the Network Interface Cards (NICs) from Fast Ethernet to gigabit.

To upgrade from Fast Ethernet to gigabit NICs

1. Upgrade the physical NIC hardware to a supported Gigabit NIC card listed on the *Hardware Compatibility Reference*.
   See “About the Hardware Compatibility Reference” on page 17.
2. Perform the in-place upgrade script on the node.
   See “Running an in-place upgrade” on page 57.
3. Edit each of the node's monitoring interfaces in the topology tree, and set the correct interface name.
   For example, `eth0`, `hme0`, or `iprb0` must be renamed to `re1000g0`.
   See the *Symantec Network Security Administration Guide* for more detailed instructions about editing monitoring interfaces in the topology tree.

   Note: Upgrading from Gigabit interfaces does not require a special conversion.

Upgrading tokens

If you have an iButton or software token in your existing installation, it will be detected during the upgrade process. If you have an existing iButton, the upgrade script offers the choice to continue using it, or to switch to a software token. If you have an existing software token, the upgrade script does not offer a choice, and instead defaults to continue using the software token.

- See “Choosing tokens” on page 94.
- See “Running an in-place upgrade” on page 57.

- See "Attaching an iButton" on page 28.

Upgrading signatures

Any existing ManHunt 3.0 R1 or R2 user-defined signatures are automatically updated during the upgrade procedure to Symantec Network Security 4.0. This occurs only during the upgrade procedure, and cannot be triggered independently of the system upgrade process. The upgrade procedure generates HTML reports that record the success of the upgrade, and list any possible modifications. Make sure to review this file after the upgrade so that you can make adjustments, if necessary.

See "Verifying success via the report log" on page 59.

Upgrading Oracle and MySQL databases

Symantec Network Security does not support the conversion of MySQL and Oracle tables from ManHunt 3.0 R1 or R2. You can archive SQL tables by a variety of methods, such as renaming or copying to another location, and then create new tables for Symantec Network Security 4.0 using the create statements.

See the *Symantec Network Security Administration Guide* for more information about managing Oracle and MySQL databases.

Note: Symantec Network Security requires a dedicated computer that is separate from any other software. To export to a MySQL or Oracle database server, you must install the database software on a separate, external machine.

Upgrading SESA Agents

You can upgrade your SESA Agent as follows:

- In-place upgrade: SESA Agent upgrades automatically during the same process as the Network Security software node upgrades.
- Backup/restore upgrade: SESA Agent upgrades automatically during the same process as the Network Security software node upgrades.
- After Network Security software node upgrade: You can manually initiate the upgrade after the Network Security software node has been upgraded, if you declined to upgrade the SESA Agent before.

Upgrading the Network Security software node without upgrading the SESA Agent can break communication with SESA. If you choose not to utilize the in-place upgrade, the connection to the SESA Management Console will be broken until you initiate the manual upgrade.

Note: Upgrading SESA Agents requires that the Network Security software node be restarted (but not rebooted) for the changes to take effect.

See the SESA documentation to find out how to back up a SESA Agent configuration and upgrade or migrate it from 1.1 to 2.0.

Upgrading clusters

This section includes the following topics:

- Upgrading a cluster of nodes
- Upgrading a node behind a NAT device

Upgrading a cluster of nodes

Symantec Network Security supports mixed-mode upgrades where ManHunt 3.0 R1 or R2 nodes can co-exist along side Symantec Network Security 4.0 nodes in the same cluster. However, while a cluster is in mixed mode, ManHunt 3.0 R1 or R2 nodes are limited to read-only availability. The new functionality of Symantec Network Security 4.0 is available only to the upgraded nodes.

Note: In a mixed-mode cluster, all Symantec Network Security 4.0 nodes have full functionality. All ManHunt 3.0 R1 or R2 nodes have read-only functionality, and cannot receive LiveUpdate or any other input.

To upgrade a cluster from ManHunt 3.0 R1 or R2

1. First upgrade the master node to Symantec Network Security 4.0.
   After this, the ManHunt 3.0 R1 or R2 console can be used to display incidents and events from both the master node (Symantec Network Security 4.0) and the slave nodes (ManHunt 3.0 R1 or R2).
2. Next, upgrade the console.
3. Finally, upgrade all slave nodes.
   During this migration period, the ManHunt 3.0 R1 or R2 nodes can be used only for collecting and displaying events. You can view, mark, and annotate incidents and events from a ManHunt 3.0 R1 or R2 slave node. No other functionality is available until the slave node is upgraded to Symantec Network Security 4.0.

Upgrading a node behind a NAT device

This section describes special considerations for upgrading a slave node that exists behind a NAT device from ManHunt 3.0 R1 or R2 to Symantec Network Security 4.0. If your cluster includes slave nodes behind a NAT device, you must make sure that communication remains open after upgrade.

To upgrade a slave node behind a NAT device

1. Upgrade the master node of the cluster and the Network Security console, in the order described in Upgrading a cluster of nodes.
2. From the Network Security console, login to the upgraded master node.
3. In the **Devices** tab, delete the NAT-ed slave object in the topology tree.
4. In the **Devices** tab, re-add the NAT-ed slave node to the topology tree.
5. Save all changes.

   See the *Symantec Network Security Administration Guide* for more detailed instructions about adding and deleting node objects to the topology tree.
6. Upgrade the slave node from ManHunt 3.0 R1 or R2 to Symantec Network Security 4.0.

Chapter 6

Licensing

This chapter includes the following topics:

- About Symantec licenses
- Installing new licenses
- Checking installed licenses
- Updating licenses
- Upgrading licensed bandwidths
- Calling for help

About Symantec licenses

All key features for the Symantec Network Security are activated by license, including software functionality and subscriptions to Product Updates.

This section includes the following topics:

- About license types
- About license dependencies

About license types

You must obtain a Symantec Network Security 4.0 license file for each node that you plan to install or upgrade. Symantec Network Security supports two types of licenses:

- Evaluation License: Non-metered (full functionality - 2Gbps allowed), time limit of 45 days, does not include a node lock
- Perpetual License: Metered (100Mbps, 200Mbps, 500Mbps, 1Gbps and 2Gbps), no time limit, includes a node lock based on IP address

About license dependencies

The Network Security console does not require a license. However, every node requires an individual license. In addition, consider the following:

- Perpetual licenses override temporary licenses, regardless of bandwidth. When perpetual licenses are installed, temporary evaluation licenses are ignored, but not removed, from the node.
- If multiple perpetual licenses exist on the same node, all valid licenses are cumulative.
- Licenses for Symantec Network Security 7100 Series appliance are invalid on Network Security software nodes.

Caution: If the Network Security console connects to an unlicensed Network Security software node, functionality is available only to activate a license. For more information, see https://licensing.symantec.com

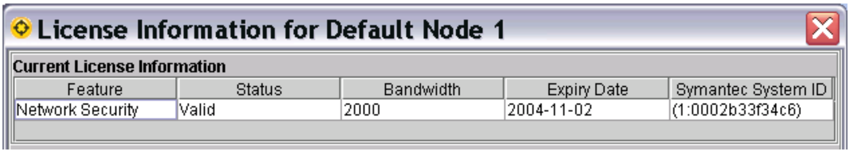
Installing new licenses

This section includes the following topics:

- Logging in to an unlicensed node
- Requesting a license file
- Installing a master node license
- Installing a slave node license
- Installing licenses from the command line

Logging in to an unlicensed node

The first time that you connect to an unlicensed Network Security software node from the Network Security console, all detection, analysis, and response capability is disabled. The Network Security console displays the License Information for Node, from which you can obtain the Symantec System ID. Note this ID so you can provide it when requesting a license from the Web site.



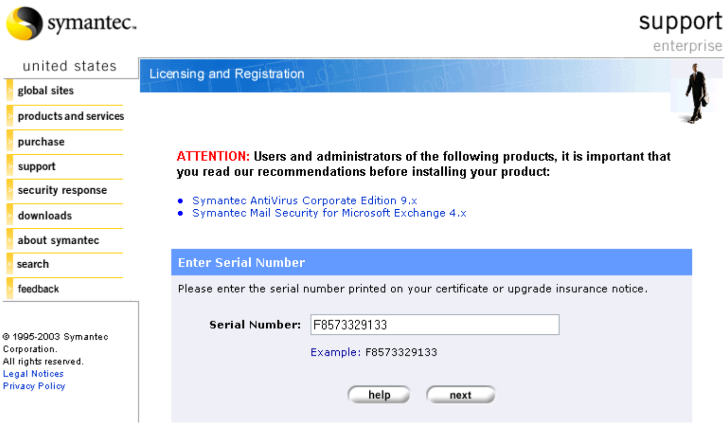
License Information for Default Node 1

Current License Information

Feature	Status	Bandwidth	Expiry Date	Symantec System ID
Network Security	Valid	2000	2004-11-02	(1:0002b33f34c6)

Requesting a license file

You must obtain a Symantec Network Security 4.0 license file for each node that you plan to install or upgrade. Request the license file from the Symantec licensing Web site at https://licensing.symantec.com



ATTENTION: Users and administrators of the following products, it is important that you read our recommendations before installing your product:

- Symantec AntiVirus Corporate Edition 9.x
- Symantec Mail Security for Microsoft Exchange 4.x

Please enter the serial number printed on your certificate or upgrade insurance notice.

Serial Number: F8573329133

Example: F8573329133

© 1995-2003 Symantec Corporation.
All rights reserved.
Legal Notices
Privacy Policy

To request the license file

1 Gather the following information:

- **Serial Number**: The Symantec Serial Number Certificate is mailed separately, and not included in the software distribution package.
- **Email Address**: Provide the email address where you will receive the license email.
- **Symantec System ID**: From the Network Security console, on the License Information for Node window, make a note of the Symantec System ID, including parentheses.

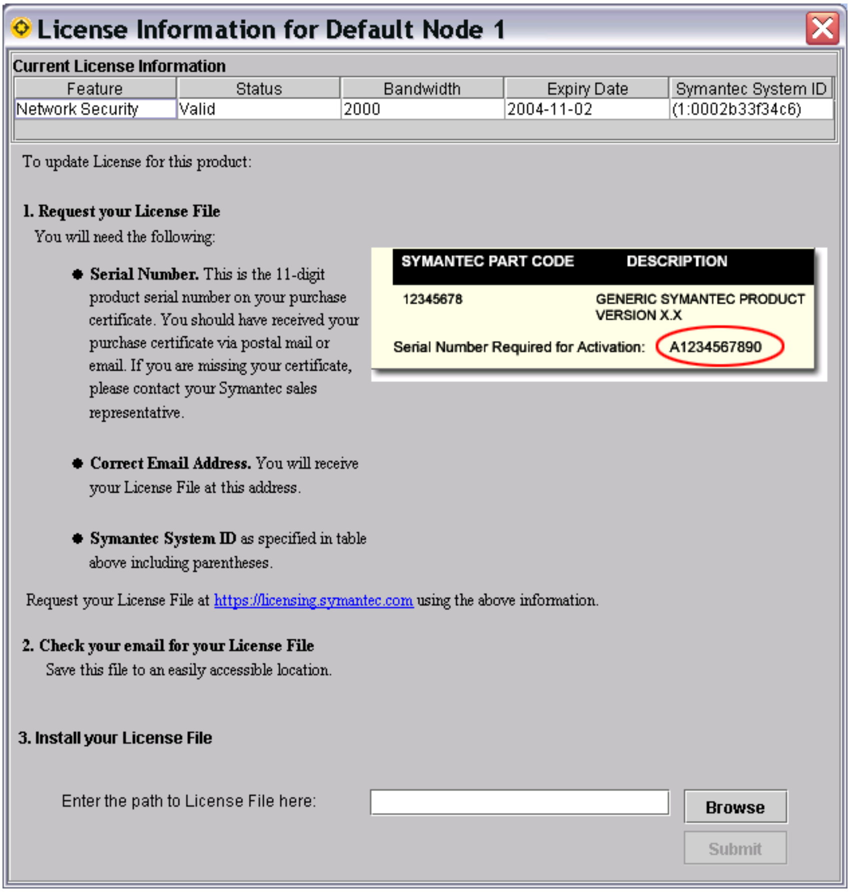
2 From your browser, access https://licensing.symantec.com

3 Follow the Web page instructions to provide the information you gathered, and request the license file.

Note: Only SuperUsers can manage licenses; Administrators, StandardUsers, and RestrictedUsers cannot. See the *Symantec Network Security Administration Guide* for more information about user permissions.

Installing a master node license

After you receive the license file, install the license from the Network Security console.



License Information for Default Node 1

Current License Information

Feature	Status	Bandwidth	Expiry Date	Symantec System ID
Network Security	Valid	2000	2004-11-02	(1:0002b33f34c6)

To update License for this product:

1. Request your License File

You will need the following:

- **Serial Number.** This is the 11-digit product serial number on your purchase certificate. You should have received your purchase certificate via postal mail or email. If you are missing your certificate, please contact your Symantec sales representative.
- **Correct Email Address.** You will receive your License File at this address.
- **Symantec System ID** as specified in table above including parentheses.

SYMANTEC PART CODE	DESCRIPTION
12345678	GENERIC SYMANTEC PRODUCT VERSION X.X

Serial Number Required for Activation: A1234567890

Request your License File at https://licensing.symantec.com using the above information.

2. Check your email for your License File

Save this file to an easily accessible location.

3. Install your License File

Enter the path to License File here:

To install the license on a master node

1 Save the license file on the Network Security console.

2 Login to the Network Security console with a SuperUser account.

When you login to an unlicensed master node, the only functionality available is to activate a license.

3 In **3. Install Your License File**, do one of the following:

- Click **Browse** to navigate to the license file and select it.
- Type the path and filename into the field.

4. Click **Submit**.
   The software indicates whether the license was installed successfully on the master node.

Note: Only SuperUsers can manage licenses; Administrators, StandardUsers, and RestrictedUsers cannot. See the *Symantec Network Security Administration Guide* for more about user permissions.

Installing a slave node license

After you receive the email containing the license file, you can install the license from the Network Security console.

To install the license on a slave node

1. Save the license file on the Network Security console.
2. Login to the Network Security console with a SuperUser account.
3. On the **Devices** tab, right-click the slave node.
4. Click **Licensing** from the pop-up menu.
5. In **3. Install Your License File**, do one of the following:
   - Click **Browse** to navigate to the license file and select it.
   - Type the path and filename into the field.
6. Click **Submit**.
   The software indicates whether the license was installed successfully on the slave node.

Installing licenses from the command line

You can install a license file from the command line, using the `mh_els_lit` tool that is available in the tools directory of the Network Security software node.

To install the license on a slave node

1. Login as root.
2. Execute the following command:
   ```
   <SNS_install_dir>/tools/mh_els_lit <license-file-path>
   ```

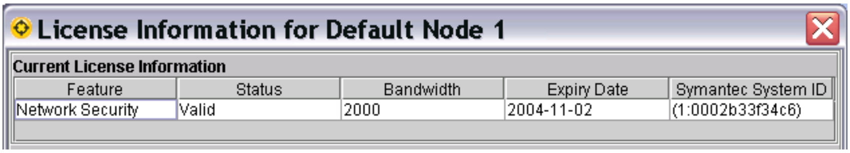
Checking installed licenses

This section includes the following topics:

- Checking license status
- Checking the Symantec System ID
- Monitoring expiration and bandwidth

Checking license status

From the Network Security console, you can check your current license to verify the status, the average monitored bandwidth, expiry dates, and other licensing information.



License Information for Default Node 1

Current License Information

Feature	Status	Bandwidth	Expiry Date	Symantec System ID
Network Security	Valid	2000	2004-11-02	(1:0002b33f34c6)

To check the license status

1. From the Network Security console, click **Admin** > **Node** > **Licensing**.
2. In **Select Node**, select the Network Security software node for which you want to retrieve licensing information, and click **OK**.
3. In **License Information**, review the following information:

Feature	Displays the node that is activated by the license.
Status	Displays the status of the license (valid, invalid, expired, or unlicensed).
Bandwidth	Displays the bandwidth for which this node was licensed. You are notified if the average monitored bandwidth exceeds the licensed bandwidth.
Expiry Date	Displays the expiration date for the license, if applicable.
Symantec System ID	Displays the Symantec System ID, an identification number for the license. Provide this number to Symantec Technical Support if you have questions regarding your license.

Checking the Symantec System ID

Each node has a unique Symantec System ID that prevents a license issued for one node from activating another node. You can find the Symantec System ID in two ways:

- From the Network Security console, click Admin > Node > Licensing.
- From the command line, use the `sym_sid` tool available in the installation package.

Monitoring expiration and bandwidth

You are notified of pending license expiration by events on the Network Security console. Similarly, you are notified of a node's average monitored bandwidth if it exceeds the licensed bandwidth. The frequency of events increases as average monitored bandwidth further exceeds the licensed bandwidth. If average monitored bandwidth exceeds licensed bandwidth by 100Mbps over a period of 7 days, you will receive further notification.

Updating licenses

Symantec Network Security 4.0 does not support upgrading a license. You must obtain a new Symantec Network Security 4.0 license file for each node that you plan to upgrade. for both the in-place upgrade and the backup/restore processes. ManHunt 3.0 R1 or R2 licenses are not valid on Network Security software nodes.

See also "Upgrading tokens" on page 66 to find out about upgrading certificates.

Upgrading licensed bandwidths

If you want to upgrade to a higher bandwidth on a node, you must install a new license on that node. Multiple licenses on the same node are cumulative. For example, to upgrade from 100Mbps to 500Mbps, a new license file with an allowed bandwidth of 400Mbps will be issued to you.

See "Installing new licenses" on page 72.

Calling for help

You can contact Symantec Global Technical Support by telephone, or at www.symantec.com/techsupp. You will be asked to supply the following:

- **Serial Number**: The Symantec Serial Number Certificate is mailed to you separately, and is not included in the Symantec Network Security software package.
- **Symantec System ID**: To find the current license information, do one of the following:
  - From the Network Security console, click **Admin** > **Node** > **Licensing**.
  - From the command line, use the `sym_sid` tool available in the installation package.

Note: Only SuperUsers can manage licenses; Administrators, StandardUsers, and RestrictedUsers cannot. See the *Symantec Network Security Administration Guide* for more about user permissions.

LiveUpdating

This chapter includes the following topics:

About Symantec™ LiveUpdate

Symantec™ LiveUpdate automates the process of delivering security and product updates to Symantec Network Security to provide real-time detection of the latest threats. Symantec Network Security provides the new LiveUpdate functionality to keep your system updated to the latest software levels in a seamless and timely manner. The Network Security console displays all available updates at any given time, and provides the LiveUpdate interface for you to selectively apply them or schedule them to be automatically applied.

Symantec Network Security now provides Security Updates, Engine Updates, and Product Updates (patches) through LiveUpdate. LiveUpdate can be configured to automatically download and apply rapid responses, or to give a threat response rating, so that you choose whether to download only, or to download and apply, based on the rating. You can configure LiveUpdate to respond automatically per cluster, per node, or per interface. You can also trigger LiveUpdate manually.

Symantec Network Security provides three kinds of LiveUpdates:

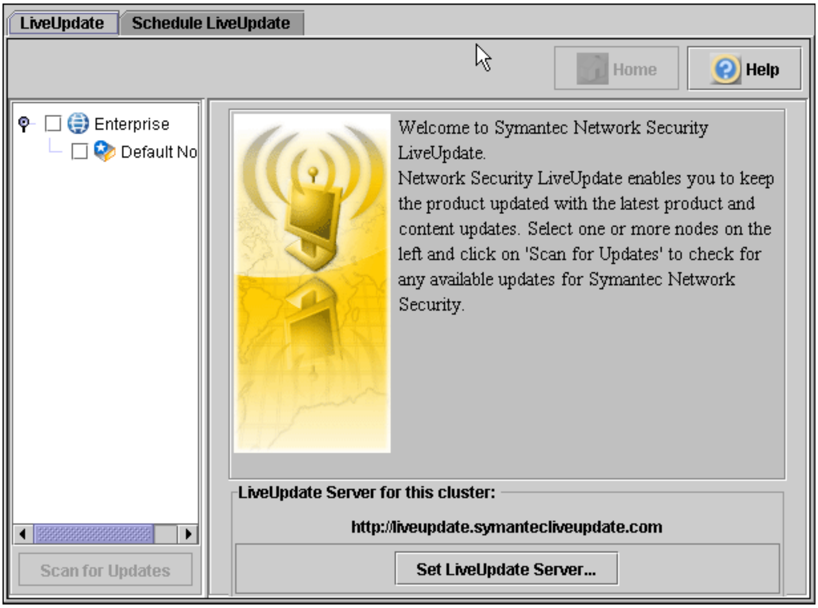
- Security Updates add detection capabilities to the product, such as event data, refinement rules, and encrypted signatures. Security Updates are cumulative. Each update includes the data from the updates before it. Some Security Updates are dependent upon Engine Updates as well. Security Updates enable you to automate the download and deployment of regular and rapid response Security Updates from Symantec Security Response, the world's leading Internet security research and support organization. Symantec Security Response provides top-tier security protection and the latest security context information, including exploit and vulnerability information, event descriptions, and event refinement rules to protect against ever-increasing threats.
- Engine Updates add cumulative features and enhancements such as sensor functionality and data. Engine Updates are cumulative. Each update includes the data from the updates before it. Some Security Updates are dependent upon Engine Updates as well. In that case, selecting one will automatically include the other.
- Software or appliance Product Updates add restoration and repair functionality (database, configuration, and database updates), patches, or minor releases. Software and appliance Product Updates are incremental, and in some cases, you can rollback a Product Update if you change your mind. You can choose any Product Update or patch level, even if it is not the latest, and each level will automatically install all previous levels. For example, you can select Patch 3, even if Patch 4 is available. However, it is not possible to select Patches 2 and 4, and skip Patch 3. When you install Patch 3, Patches 1 and 2 are automatically included.

Scanning for available updates

Symantec Network Security provides a list of all available LiveUpdates in the Network Security console.

To view available updates

1 In the Network Security console, click **Admin** > **LiveUpdate**.



Welcome to Symantec Network Security LiveUpdate.
Network Security LiveUpdate enables you to keep the product updated with the latest product and content updates. Select one or more nodes on the left and click on 'Scan for Updates' to check for any available updates for Symantec Network Security.

LiveUpdate Server for this cluster:

http://liveupdate.symantecliveupdate.com

2 In the left pane, select the relevant nodes.

3 On the **LiveUpdate** tab, click **Scan For Updates**.

Note: SuperUsers and Administrators can view LiveUpdate using the Network Security console; StandardUsers and RestrictedUsers cannot. See *Symantec Network Security Administration Guide* for more about user permissions.

Applying updates

The Network Security console provides a way to apply automatic updates to the system easily.

To apply automatic updates

1 In the Network Security console, click **Admin** > **LiveUpdate**.

2 In the left pane, select the nodes to receive updates.

3 On the **LiveUpdate** tab, click **Scan For Updates**.

4 In **Available Updates**, do one of the following:

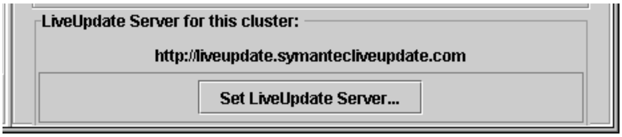
- Click **Select All** to select the entire list.
- Click **Clear All** to deselect the entire list.
- Click each update to select it individually.

5 Click **Apply Updates** to activate the selection.

Note: SuperUsers and Administrators can apply updates using the Network Security console; StandardUsers and RestrictedUsers cannot. See *Symantec Network Security Administration Guide* for more about user permissions.

Setting a LiveUpdate server

Symantec Network Security supports two server options. You can use either the default LiveUpdate server, or establish an alternative LiveUpdate server.



LiveUpdate Server for this cluster:

http://liveupdate.symantecliveupdate.com

This section includes the following topics:

- Setting a LiveUpdate server
- Obtaining LiveUpdate packages
- Making the host name resolvable

Setting a LiveUpdate server

If you establish an alternative server, you must use this procedure when you add new nodes to a cluster. This procedure sets each new node to be receptive to the alternative LiveUpdate server. If you add a new node to the cluster without taking this step, the new node will automatically use the default LiveUpdate server for the cluster, rather than the alternative.

To set the LiveUpdate server

1 In the Network Security console, click **Admin** > **LiveUpdate**.

2 On the **LiveUpdate** tab, click **Set LiveUpdate Server**.

3 In **LiveUpdate Server Configuration**, provide the following information:

- Enter the **Hostname** or IP address of the LiveUpdate server.
- Select the **Type** from the pull-down list.
- If you selected the **FTP** type, enter the **Username** and **Password**.

- Click **OK**.

Note: SuperUsers and Administrators can establish a LiveUpdate server using the Network Security console; StandardUsers and RestrictedUsers cannot. See *Symantec Network Security Administration Guide* for more about permissions.

Obtaining LiveUpdate packages

If you prefer not to maintain browser access on a node for security reasons, you can use the `luadmin` command-line tool to get the LiveUpdate packages and check for updates. Download the tool and the relevant documentation from the Symantec LiveUpdate Web site:

http://www.symantec.com/techsupp/files/lu/lu.html

If you choose to configure your own LiveUpdate server, consider the following:

- Engine Updates are cumulative. Therefore, keep only the latest Engine Updates on the server. For example, if there are 10 Engine Updates, keep the 10th, not Engine Update 1-10. Remove Engine Update 10 as soon as Engine Update 11 is released.
- Product Updates or patches, on the other hand, are not cumulative, even though they are dependent. For example, even if you want only Product Update4, keep Product Updates 1-3 on the internal LiveUpdate server.

Note: Contact Support at http://www.symantec.com/techsupp/ if the LiveUpdate server does not function properly.

Making the host name resolvable

For either a default LiveUpdate server or an alternative LiveUpdate server, verify that the server has a name that DNS can resolve. Both types of servers require a DNS-resolvable name. If the host name is not known to the DNS server, you can make it locally resolvable by adding it to the `/etc/hosts` file.

To make the host name resolvable

1. Login to the node as root.
2. Edit the `/etc/hosts` file by adding the host name to the `localhost` line.
   For example:
   ```
   127.0.0.1  localhost.localdomain  localhost  <hostname>
   ```
3. Save the file and exit.

Scheduling updates

This section describes the following topics:

- Adding or editing automatic updates
- Deleting automatic update schedules
- Reverting automatic update schedules

Adding or editing automatic updates

The Network Security console provides a way to schedule automatic updates. You can set only one schedule per node. If you add a second schedule to the same node, it will override the first.

To schedule or reschedule automatic updates

1. In the Network Security console, click **Admin** > **LiveUpdate**.
2. On the **Schedule LiveUpdate** tab, do one of the following:
   - Click **Add** to create a new schedule.
   - Click an existing schedule, and click **Edit** to change the schedule.
   - Click an existing schedule, and click **Delete** to remove the schedule.
3. In **LiveUpdate Frequency**, provide the following information:
   - In **Check for Updates Every**, select Week, Day, or Hour from the pull-down list.
   - In **Day To Run**, select the day of the week from the pull-down list.
   - In **Hour To Run**, select a time from the pull-down list, and click a radio button to select AM or PM.
   - In **Auto Install Options**, click the checkbox if you want Engine Updates to be automatically installed, and Security Updates that meet policy rules to be applied.
4. In **Applies To Nodes**, click **Edit**.
5. In **Select Nodes**, click each node to receive updates, and click **OK**.
6. In **LiveUpdate Schedule**, click **OK**.
7. In the **Schedule LiveUpdate** tab, do one of the following:
   - Click **Save** to preserve your choices.
   - Click **Revert** to undo your choices.

Note: SuperUsers and Administrators can schedule automatic updates using the Network Security console; StandardUsers and RestrictedUsers cannot. See *Symantec Network Security Administration Guide* for more about permissions.

Deleting automatic update schedules

This section describes how to delete automatic update schedules easily.

To delete an automatic update schedule

1 In the Network Security console, click **Admin** > **LiveUpdate**.

2 On the **Schedule LiveUpdate** tab, select an existing schedule.

3 Click **Delete** to remove the schedule.

Reverting automatic update schedules

The Network Security console provides a way to revert changes to automatic update schedules easily. This procedure reverts all changes. To revert one change out of a number of changes, save them, and delete the one.

To revert changes to an automatic update schedule

1 In the Network Security console, click **Admin** > **LiveUpdate**.

2 On the **Schedule LiveUpdate** tab, click **Revert** to undo all changes.

Backing up LiveUpdate configurations

The Network Security console provides a way to customize Symantec Network Security to allow for internal LiveUpdate servers. See the LiveUpdate documentation for this information.

We recommend that you back up the `liveupdate.conf` file if you customize it. Because the Network Security console Manage Backup procedures do not include this file, you can provide backups by copying this file manually and storing it in a safe location.

If you uninstall Symantec Network Security, the procedure completely uninstalls LiveUpdate as well, and removes any configuration for the LiveUpdate client. If you customized the `liveupdate.conf` file to allow for alternative LiveUpdate servers, you must restore it after reinstalling. So make sure to back up the customization.

Note: SuperUsers can check and apply updates using the Network Security console; Administrators, StandardUsers, and RestrictedUsers cannot. See *Symantec Network Security Administration Guide* for more about permissions.

Integrating with SESA

This appendix includes the following topics:

About the SESA Bridge

The Symantec Network Security SESA™ Bridge allows you to send events from Symantec Network Security™ 4.0 to the Symantec Enterprise Security Architecture (SESA) 2.0 Management Console.

SESA is an underlying software infrastructure that integrates multiple Symantec and third-party products to provide flexible control of security within organizations. It protects your IT infrastructure from malicious code, intrusions, and blended threats. You can monitor and manage security-related events through the SESA Console. However, you cannot configure Symantec Network Security from the SESA Management Console.

Symantec Network Security can export event data to SESA using the SESA Bridge. The SESA Bridge is not required to use Symantec Network Security in native mode. You can install the Bridge to software nodes by running the Bridge installation script located in the `<SNS_install_dir>/install/sesabridge` directory. All configuration of the Bridge is done through the Network Security console.

Requirements for the SESA Bridge

You will need the following:

- Symantec Network Security installed on a dedicated computer, or on a Symantec Network Security 7100 Series appliance
- SESA 2.0
- SESA Integration Package (SIP) installed on the SESA Manager, to register Symantec Network Security with SESA 2.0
- SESA Bridge installed on each software or appliance node that will send events to SESA
- SESA Agent

Installing the SESA Bridge

If you want to maintain SESA Bridge functionality, you can find the install and uninstall scripts in the `<SNS_install_dir>/install/sesabridge` directory. The `/usr/SNS` is the default install directory. You can choose to install the software in another location, and direct the SESA Bridge scripts accordingly.

This section includes the following topics:

- Making the host name resolvable
- Making the SIP file available on the SESA manager
- Installing the SESA Bridge

Making the host name resolvable

Before installation, verify that DNS can resolve the host name. The SESA Agent installer requires a DNS-resolvable host name. If the host name is not known to the DNS server, you can make it locally resolvable by adding it to the `/etc/hosts` file.

To make the host name resolvable

1. Login to the node as root.
2. Edit the `/etc/hosts` file by adding the host name to the `localhost` line.
   For example:
   ```
   127.0.0.1  localhost.localdomain  localhost  <hostname>
   ```
3. Save the file and exit.

Making the SIP file available on the SESA manager

Before installation, verify that the Symantec Network Security SESA Integration Package (SIP) file is available on the SESA Manager. The SIP file is available on the Management Console CD. You can access it directly from the CD or copy it to the SESA Manager.

This section includes the following topics:

- Accessing the SIP file
- Copying the SIP file

Accessing the SIP file

This section describes how to access the SIP file directly from the CD.

To access the SIP file directly from the CD

1 Insert the Management Console CD into the CD drive on the SESA manager.

2 Follow the instructions in the SESA documentation for the **Register SESA Integrated Product** procedure on the SESA manager.

3 When the instructions in the wizard ask for the SESA Integration Package to install, navigate to the file location on the CD:

```
install/console/sesa/NetworkSecurity_4_0.sip
```

Copying the SIP file

This section describes how to copy the SIP file onto the SESA manager.

To copy the SIP file onto the SESA Manager

1 Insert the Management Console CD into the CD drive on the SESA manager.

2 Open the CD drive to access the CD.

3 Browse to the `install/console/sesa` folder.

4 Click and drag the SIP file `NetworkSecurity_4_0.sip` to a folder on the SESA manager.

Installing the SESA Bridge

The `install-sesabridge.sh` script installs both the SESA Agent and other software included in the SESA Bridge.

See the SESA documentation for more information about SESA.

To install the SESA Bridge

1. Login as root.
2. Execute the following command:
   ```
   cd <SNS_install_dir>/install/sesabridge
   ```
3. Execute the following command:
   ```
   ./install_sesabridge.sh
   ```
4. When warned that Symantec Network Security processes will stop, do one of the following:
   - Type `y` to continue installing the SESA Bridge, and press **Enter**.
   - Type `n` to abort the procedure, and press **Enter**.
5. When asked for the SESA manager, do one of the following:
   - Enter the IP address of the SESA manager if you use Anonymous SSL.
   - Enter the hostname of the SESA manager if you use Authenticated SSL.
6. When asked which port to use to connect to the primary SESA manager, do one of the following:
   - Press **Enter** to accept the default port `443`.
   - Type an alternative port number, and press **Enter**.
7. When asked which IP address to use for the CIMOM, do one of the following:
   - Press **Enter** to accept the default IP address.
   - Type an alternative IP address, and press **Enter**.
8. When asked which port to use for the CIMOM, do one of the following:
   - Press **Enter** to accept the default port `5998`.
   - Type an alternative port number, and press **Enter**.
9. When asked for the servlet prefix, do one of the following:
   - Press **Enter** to accept the default `/sesa/servlet/` prefix.
   - Type an alternative prefix, and press **Enter**.
10. Exit when the prompt indicates that the SESA Bridge configuration is complete and the node is restarting.

Uninstalling the SESA Bridge

The uninstall procedure removes both the SESA Agent and related Bridge software. To uninstall the SESA Bridge and SESA Agent, you must stop and restart Symantec Network Security.

To uninstall the SESA Bridge

1. Login as root.
2. Execute the following command:
   ```
   cd <SNS_install_dir>/install/sesabridge
   ```
3. Execute the following command:
   ```
   ./uninstall_sesabridge.sh
   ```
4. When warned that Symantec Network Security processes will stop, do one of the following:
   - Type `y` to continue uninstalling the SESA Bridge.
   - Type `n` to abort the procedure.
5. Exit when the prompt indicates that the SESA Bridge is uninstalled.

Managing the SESA Bridge

This section includes the following topics:

- Starting the SESA Agent manually
- Stopping the SESA Agent manually

Starting the SESA Agent manually

You can start the SESA Agent manually from the command line. The SESA Agent starts automatically when you install the SESA Bridge, but if you manually stop it, then you must restart it again to send events to the SESA manager.

To start the SESA Agent manually

1. Login as root.
2. Execute the following command:
   ```
   /etc/init.d/sesaagentd start
   ```

Stopping the SESA Agent manually

You can stop the SESA Agent manually from the command line.

To stop the SESA Agent manually

1. Login as root.
2. Execute the following command:
   ```
   /etc/init.d/sesaagentd stop
   ```

Using iButtons

This chapter includes the following topics:

- See “Choosing tokens” on page 94.
- See “Installing or replacing tokens” on page 94.
- See “Installing or replacing hardware tokens” on page 95.
- See “Disabling tokens” on page 96.
- See “Using iButtons” on page 96.

About hardware or software tokens

This section describes the software token and the hardware token (iButton™), the two types of tokens that Symantec Network Security uses to sign log files.

About software tokens

The main function of the software token is to provide basic log signing functionality with some limited tamper protection.

About hardware tokens

The iButton (hardware token) is an optional component that is attached to a Network Security software node to provide protection against falsification of log records, and to authenticate signatures so that log data can be used against an intruder. The iButton also provides the following benefits:

- Signs non-repudiation logs, giving you the ability to prove that the logs are not tampered with
- Provides stronger session keys for system communication

- Enables cryptographic services to be off-loaded to a FIPS 140-1 token (a secure module that is evaluated at high rigor levels)

Communication can be secured with the use of the iButton token and a Network Security signature certificate. The iButton acts as a digital credential to sign data and authenticate that it has not been tampered with. The iButton stores the private key portion of the certificate to safeguard the private key against being stolen or compromised. A software token is available as an alternative to the iButton.

Choosing tokens

Symantec Network Security provides two types of tokens used to sign log files: the software token and the hardware token (also called the iButton™). During installation, you can choose either an iButton or a software token. At any time after installation, you can change that setting.

During the upgrade procedure, if you used an iButton in the previous installation, you can choose to continue or to switch to a software token. If you used a software token in the previous installation, the upgrade procedure will default to continue using a software token.

Both software tokens and iButtons can be installed during the installation process. After Symantec Network Security is up and running, you can use the `<SNS_install_dir>/token_intall.sh` and `token_remove.sh` scripts to switch.

Installing or replacing tokens

This section includes the following topics:

- Installing software tokens
- Installing or replacing hardware tokens

Installing software tokens

You can add or remove both hardware and software tokens after installation by using the `token-install.sh` and `token-remove.sh` tools in the `install` subdirectory. Only one software token can exist on the system. If you install a second software token, the previous token will be overwritten, and you will not be able to verify logs signed by the previous token.

Note: Before installing a software token, you must first remove a hardware token, if you have one. If you have a hardware token installed, it is the default. See "Disabling tokens" on page 96.

To install a software token

1. In the `<SNS_install_dir>` directory, execute the following command:

   ```
   ./token-install.sh
   ```

2. To indicate that you want to install a software token, type `y` and press **Enter**. The software token and certificate are generated.

   Caution: Although you can install a new software token if you did not have one previously installed, you cannot reinstall or restore an old software token unless you previously backed it up.

Installing or replacing hardware tokens

You can add or remove both hardware and software tokens after installation by using the `token-install.sh` and `token-remove.sh` tools.

If you had an iButton in your previous installation that has expired, you must either replace the iButton, or disable it and revert to the software token. This section describes how to replace the iButton.

See "Checking iButton status" on page 97.

See "Disabling tokens" on page 96.

Note: The system does not prevent you from having both a hardware and a software token installed simultaneously. Symantec Network Security will always default to the hardware token under this circumstance.

To install or replace the iButton

1. Stop the Network Security software node by executing the following command:

   ```
   <SNS_install_dir>/stop
   ```

2. Remove the old iButton and replace it with the new iButton.
3. Initialize the iButton by executing the following command:

   ```
   <SNS_install_dir>/token-install.sh
   ```

4. Enter the path to the iButton device when prompted.

5. Restart the Symantec Network Security software by doing one of the following:
   - Reboot the machine.
   - Execute the following command:

     ```
     <SNS_install_dir>/start
     ```

Disabling tokens

You can disable a hardware or software token at any time, and install another token.

To disable or remove a token

1. Stop the Network Security software node by executing the following command:

   ```
   <SNS_install_dir>/stop
   ```

2. In the `<SNS_install_dir>` directory, execute the following command:

   ```
   ./token-remove.sh
   ```

3. When asked if you want to remove the hardware token, type `y` and press **Enter**. The hardware token installation will be removed.
4. Use the following tool to add a software token:

   ```
   token-install.sh
   ```

   See “Installing or replacing tokens” on page 94.

   Caution: Once a software token is removed, logs signed with that token cannot be verified. There is no way to reinstall a software token, unless it was backed up.

Using iButtons

You can use iButtons on Network Security software nodes only; the iButton is unnecessary for 7100 Series appliance nodes. This section describes solutions to problems with the iButton, a hardware token that stores the private key portion of the Network Security signature certificate to safeguard the private key against being stolen or compromised. The iButton also confirms the identity of a node.

This section describes the following:

- Checking iButton status
- Reinitializing an iButton

- Changing the iButton communication port
- iButton signatures under high loads
- Reading iButton errors and solutions

Checking iButton status

The Incidents tab of the Network Security console displays notifications of the impending expiration well before the iButton expires. Contact http://www.symantec.com/techsupp/enterprise/ when your iButton is about to expire. Replace it before it expires to ensure that the log files continue to be signed and it can continue to perform its authentication and data hashing functions.

Reinitializing an iButton

If the log displays errors indicating that the iButton is not working properly, or if the PIN has become corrupted, reinitialize the iButton. Use the `<SNS_install_dir>/token_intall.sh` and `token_remove.sh` scripts to reinitialize both software tokens and iButtons.

See "Installing or replacing hardware tokens" on page 95.

Changing the iButton communication port

If you want to move the location of the iButton, such as from `ttyb` to `ttya`, you can edit the `ibutton.loc` file.

To change the communication port

1. Change directories to the following:

   ```
   <SNS_install_dir>/dbs
   ```

2. Execute the following command:

   ```
   printf “%s” “/dev/ttya” > ibutton.loc
   ```

iButton signatures under high loads

If iButton signatures fail or are incorrect (`fail verify check`), the improper signatures are not logged. The iButton will simply try again at the next signing interval. Symantec Network Security keeps a running hash of data records and re-initializes this hash only if a signature is properly generated and written to the logs.

Reading iButton errors and solutions

The following table describes the solutions to errors that can appear in the Network Security log files, indicating that the iButton is not working properly:

Error	Solution
`ERR_NO_JIBS_FOUND 0xF000`	Ensure that the iButton is securely seated inside the caddy.
`ERR_BAD_JIB_ROM 0xF100`	Reinitialize the iButton.
`ERR_JIB_NOT_FOUND 0xF200`	Ensure that the iButton is securely seated inside the caddy.
`ERR_ADAPTER_NOT_FOUND 0xF300`	Ensure that the iButton caddy is properly attached to the appropriate communication port.
`ERR_COMM_FAILURE 0xF400`	Ensure that the proper serial port is selected; for example, `/dev/ttyb` on Solaris, or `/dev/cuao` on Linux.

Reimaging iForce

This appendix includes the following topics:

About iForce

The iForce IDS Appliance provides a solution that extends the network's ability to detect intrusions by implementing advanced protocol anomaly detection, traffic state profiling, and statistical flow analysis. Originally released with Symantec ManHunt 3.0 software, you can now upgrade an iForce IDS Appliance to Symantec Network Security 4.0 if Symantec ManHunt 3.0 software was previously configured and running.

Upgrading iForce

You can upgrade an iForce IDS Appliance to Symantec Network Security 4.0 if Symantec ManHunt 3.0 software was previously configured and running.

To upgrade remotely

1. On the Symantec Network Security 4.0 CD, in the iForce directory, select the following three files:
   - `SYMCmh40.tar`
   - `SYMCmhapp40.tar`
   - `upgrade.sh`
2. Use SCP to copy all three files to a temporary directory on the iForce appliance.
3. On the iForce appliance, login as `root`.

4 Change directories to the temporary directory containing the upgrade files.

5 Execute the following command:

```
sh upgrade.sh
```

6 On the iForce appliance, login as `secadm`.

7 Execute the following command, which will take you step-by-step through the upgrade process:

```
configure
```

Reimaging iForce

In the event that iForce crashes, you can restore the iForce IDS Appliance using your original iForce 2.1 reinstallation CD-ROM. This reinstalls Symantec ManHunt 3.0. You can then follow the standard upgrade procedure to bring the appliance to ManHunt 3.0 R1, and then to Symantec Network Security 4.0.

To restore the iForce IDS Appliance to the factory settings

1 Insert the iForce emergency reinstall CD into the CD-ROM drive.

2 Depending on how you plan to connect the iForce IDS Appliance, do one of the following:

- Insert the KVM boot floppy.
- Insert the serial boot floppy.

3 Power on the iForce IDS Appliance and wait for the **Solaris Device Configuration Assistant** screen to appear.

4 In **Solaris Device Configuration Assistant**, press **F2**.

5 In **Bus Enumeration**, press **Enter**.

6 In **Identified Devices**, press **F2**.

7 In **Boot Solaris**, use the arrow key to move down to the CD option.

8 Press the spacebar to select **CD**

To verify that you have selected it, look for an **X** displayed next to **CD**. If you select the wrong option, you can deselect the incorrect choice by pressing the spacebar again.

9 Press **F2**.

10 Wait 5 to 15 minutes while the system images, and the iForce IDS Appliance reboots.

11 After the iForce IDS Appliance has rebooted, check the screen description of the node hardware, and do one of the following:

- If it is correct, type y and press **Enter**.
- If it is incorrect, type n and press **Enter**.

Note: If the hardware description is still inaccurate after rebooting, contact Technical Support. See "Contacting Technical Support" on page 3.

12 After the iForce IDS Appliance reboots again, you can do any of the following:

- Configure the fresh machine.
- Restore the configuration and data from previous backups.
- Run the ManHunt upgrade procedure to upgrade to ManHunt 3.0 R1.
- Run the Symantec Network Security upgrade procedure to upgrade to Symantec Network Security 4.0.

Index